商用密码应用安全性评估从业人员考核参考题库

序号	题型	题干	选项A	选项B	选项C	选项D
1	单项选择题	党的二十大主题是：高举中国特色社会主义伟大旗帜，全面贯彻新时代中国特色社会主义思想，弘扬伟大建党精神，自信自强、守正创新，（ ）、勇毅前行，为全面建设社会主义现代化国家、全面推进中华民族伟大复兴而团结奋斗。	踔厉奋发	奋勇向前	赓续前向	奋楫争先
2	单项选择题	中国共产党第二十次全国代表大会，是在全党全国各族人民迈上全面建设社会主义现代化国家新征程、向（ ）奋斗目标进军的关键时刻召开的一次十分重要的大会。	第一个百年	第二个百年	第三个百年	第四个百年
3	单项选择题	党的二十大报告指出，面对突如其来的新冠肺炎疫情，我们坚持人民至上、（ ），坚持动态清零不动摇，开展抗击疫情人民战争、总体战、阻击战，最大限度保护了人民生命安全和身体健康，统筹疫情防控和经济社会发展取得重大积极成果。	精神至上	原则至上	自信至上	生命至上
4	单项选择题	党的二十大报告指出，我们经过接续奋斗，实现了小康这个中华民族的千年梦想，近（ ）农村贫困人口实现脱贫，九百六十多万贫困人口实现易地搬迁。	百万	千万	一亿	十亿

5	单项选择题	党的二十大报告指出，我国国内生产总值从五十四万亿元增长到一百一十四万亿元，我国经济总量占世界经济的比重达百分之十八点五，提高七点二个百分点，稳居世界（　）。	第一	第二	第三	第四
6	单项选择题	党的二十大报告指出，我国基础研究和原始创新不断加强，一些关键核心技术实现突破，战略性新兴产业发展壮大，进入（　）国家行列。	实践型	发展型	科研型	创新型
7	单项选择题	党的二十大报告指出，我国成为一百四十多个国家和地区的主要贸易伙伴，货物贸易总额居（），吸引外资和对外投资居世界前列，形成更大范围、更宽领域、更深层次对外开放格局。	世界第一	世界第二	世界第三	世界第四
8	单项选择题	党的二十大报告指出，贯彻（　），以坚定的意志品质维护国家主权、安全、发展利益，国家安全得到全面加强。	新时代国家安全观	总体国家安全观	国家安全体系	国家安全教育
9	单项选择题	党的二十大报告指出，全面准确推进“一国两制”实践，坚持“一国两制”、“港人治港”、“澳人治澳”、（　）的方针。	区域自治	全面自治	高度自治	基本自治
10	单项选择题	党的二十大报告指出，“打虎”、“拍蝇”、（　）多管齐下，反腐败斗争取得压倒性胜利并全面巩固，消除了党、国家、军队内部存在的严重隐患。	打蚊	猎狐	除蚁	捕狼
11	单项选择题	党的二十大报告指出，中国共产党为什么能，中国特色社会主义为什么好，归根到底是马克思主义行，是（　）的马克思主义行。	中国化时代化	时代化理论化	理论化现代化	中国化现代化
12	单项选择题	党的二十大报告指出，未来（　）是全面建设社会主义现代化国家开局起步的关键时期。	三年	五年	十年	二十年

13	单项选择题	党的二十大报告指出，我国发展进入战略机遇和风险挑战并存、不确定难预料因素增多的时期，各种“黑天鹅”、“（　）”事件随时可能发生。	黄犀牛	红天鹅	灰犀牛	白天鹅
14	单项选择题	党的二十大报告指出，完善个人所得税制度，规范（ ），规范财富积累机制，保护合法收入，调节过高收入，取缔非法收入。	收入来源	收入分配秩序	法律法规	薪资水平
15	单项选择题	党的二十大报告指出，我们要推进（ ），坚持山水林田湖草沙一体化保护和系统治理，统筹产业结构调整、污染治理、生态保护、应对气候变化，协同推进降碳、减污、扩绿、增长，推进生态优先、节约集约、绿色低碳发展。	美丽中国建设	生态环境整治	乡村振兴	环境保护
16	单项选择题	党的二十大报告指出，如期实现建军一百年奋斗目标，加快把人民军队建成世界一流军队，是全面建设社会主义现代化国家的（ ）。	方针政策	战略要求	使命	安全保障
17	单项选择题	党的二十大报告指出，我们对新时代党和国家事业发展作出科学完整的战略部署，提出实现中华民族伟大复兴的中国梦，以（　）推进中华民族伟大复兴，统揽伟大斗争、伟大工程、伟大事业、伟大梦想，明确“五位一体”总体布局和“四个全面”战略布局。	创新式发展	中国式发展	全面现代化	中国式现代化
18	单项选择题	党的二十大报告指出，我们全面加强党的领导，明确中国特色社会主义最本质的特征是（　）。	坚持马克思主义	坚持人民民主专政	中国共产党领导	密切联系群众
19	单项选择题	党的二十大报告指出，（　）是社会主义民主政治的本质属性，是最广泛、最真实、最管用的民主。	全方位人民民主	全覆盖人民民主	全参与人民民主	全过程人民民主
20	单项选择题	党的二十大报告指出，着力推进（　），推动经济实现质的有效提升和量的合理增长。	共同富裕	全面乡村振兴	城乡融合和区域协调发展	基层民主建设

21	单项选择题	党的二十大报告指出，十年来，我们深入贯彻（ ）的发展思想，在幼有所育、学有所教、劳有所得、病有所医、老有所养、住有所居、弱有所扶上持续用力，人民生活全方位改善。	人民至上	以人民为中心	以发展为中心	深化改革
22	单项选择题	党的二十大报告指出，我们党作为世界上最大的马克思主义执政党，要始终赢得人民拥护、巩固长期执政地位，必须时刻保持（ ）的清醒和坚定。	解决大党独有难题	赶考	为民造福，执政为民	全心全意为人民服务
23	单项选择题	党的二十大报告指出，全面从严治党永远在路上，党的自我革命永远在路上，决不能有（ ）的情绪，必须持之以恒推进全面从严治党，深入推进新时代党的建设新的伟大工程，以党的自我革命引领社会革命。	疲劳厌战	松劲歇脚	松劲歇脚、疲劳厌战	疲劳厌战、松劲歇脚
24	单项选择题	党的二十大报告指出，十年来，我们完善外交总体布局，积极建设覆盖全球的伙伴关系网络，推动构建（ ）。	现代国际关系	人类命运共同体	多边外交关系	新型国际关系
25	单项选择题	党的二十大报告指出，必须更好发挥法治固根本、稳预期、利长远的保障作用，在（ ）上全面建设社会主义现代化国家。	人治轨道	德治轨道	法治轨道	政治轨道
26	单项选择题	党的二十大报告指出，要加快发展方式（ ），深入推进环境污染防治，提升生态系统多样性、稳定性、持续性，积极稳妥推进碳达峰碳中和。	平稳转型	智能转型	绿色转型	快速转型
27	多项选择题	党的二十大报告指出，我们开展了史无前例的反腐败斗争，以“得罪千百人、不负十四亿”的使命担当祛疴治乱，不敢腐、（ ）、一体推进。	不可腐	不能腐	不想腐	不愿腐

28	多项选择题	党的二十大报告指出，教育、科技、人才是全面建设社会主义现代化国家的（　）支撑。	基础性	总领性	战略性	决定性
29	多项选择题	党的二十大报告指出，坚守中华文化立场，提炼展示中华文明的精神标识和文化精髓，加快构建中国话语和中国叙事体系，讲好中国故事、传播好中国声音，展现（　）的中国形象。	可信	可爱	可敬	可靠
30	多项选择题	党的二十大报告指出，“（　）”方针是实现两岸统一的最佳方式，对两岸同胞和中华民族最有利。	和平统一	一国两制	和平共处	保持现状
31	多项选择题	党的二十大报告指出，加快建设贸易强国，营造（　）一流营商环境。	市场化	法治化	国际化	区域化
32	多项选择题	党的二十大报告指出，健全总揽全局、协调各方的党的领导制度体系，完善党中央重大决策部署落实机制，确保全党在（　）上同党中央保持高度一致，确保党的团结统一。	政治立场	政治方向	政治原则	政治道路
33	多项选择题	党的二十大报告指出，坚持（　），树立选人用人正确导向，选拔忠诚干净担当的高素质专业化干部，选优配强各级领导班子，加强干部斗争精神和斗争本领养成，激励干部敢于担当、积极作为。	德才兼备	以德为先	五湖四海	任人唯贤
34	多项选择题	党的二十大报告指出，锲而不舍落实中央八项规定精神，持续深化纠治“四风”，重点纠治（　）、（　），坚决破除特权思想和特权行为。	享乐主义	形式主义	官僚主义	躺平主义

35	多项选择题	党的二十大报告指出，广大青年要坚定不移听党话、跟党走，怀抱梦想又脚踏实地，敢想敢为又善作善成，立志做（　）、能吃苦、肯奋斗的新时代好青年，让青春在全面建设社会主义现代化国家的火热实践中绽放绚丽之花。	有理想	敢担当	有决心	有信念
36	多项选择题	党的二十大报告指出，加快军事理论现代化、军队组织形态现代化、军事人员现代化、武器装备现代化，提高捍卫（　）战略能力，有效履行新时代人民军队使命任务。	国家主权	安全	发展利益	人民权利
37	多项选择题	党的二十大报告指出，加快发展方式绿色转型。推动经济社会发展（ ）是实现高质量发展的关键环节。	绿色化	节能化	节约化	低碳化
38	多项选择题	党的二十大报告指出，坚持（ ），持续深入打好蓝天、碧水、净土保卫战。	精准治污	合理治污	科学治污	依法治污
39	多项选择题	党的二十大报告指出，强化社会治安整体防控，推进扫黑除恶常态化，依法严惩群众反映强烈的各类违法犯罪活动。发展壮大群防群治力量，营造见义勇为社会氛围，建设（ ）的社会治理共同体。	人人参与	人人有责	人人尽责	人人享有
40	多项选择题	党的二十大报告指出，坚持（　）一体建设，全面推进科学立法、严格执法、公正司法、全民守法，全面推进国家各方面工作法治化。	法治国家	法治政府	法治社会	法治人民
41	多项选择题	党的二十大报告指出，弘扬以伟大建党精神为源头的中国共产党人精神谱系，用好红色资源，深入开展社会主义核心价值观宣传教育，深化（ ）教育，着力培养担当民族复兴大任的时代新人。	爱国主义	集体主义	社会主义	安全主义

42	多项选择题	党的二十大报告指出，我们要实现好、维护好、发展好最广大人民根本利益，紧紧抓住人民最关心最直接最现实的利益问题，坚持（　）。	尽力而为	量力而行	深入群众	深入基层
43	多项选择题	“六个必须坚持”是指，必须坚持人民至上、必须坚持（　）、必须坚持守正创新、必须坚持（　）、必须坚持系统观念、必须坚持胸怀天下。	自信自强	自信自立	问题导向	问题意识
44	多项选择题	“四个全面”战略布局是指,（　）、（　）、（　）、全面从严治党。	全面建设社会主义现代化国家	全面建成社会主义现代化国家	全面深化改革	全面依法治国
45	多项选择题	党的二十大报告指出，我们坚持绿水青山就是金山银山的理念，污染防治攻坚向纵深推进，（　）发展迈出坚实步伐，生态环境保护发生历史性、转折性、全局性变化。	绿色	节能	循环	低碳
46	多项选择题	党的二十大报告指出，经过不懈努力，党找到了自我革命这一跳出治乱兴衰历史周期率的第二个答案，（　）能力显著增强，管党治党宽松软状况得到根本扭转，风清气正的党内政治生态不断形成和发展，确保党永远不变质、不变色、不变味。	自我净化	自我完善	自我革新	自我提高
47	多项选择题	党的二十大报告指出，我们必须坚持解放思想、实事求是、与时俱进、求真务实，一切从实际出发，着眼解决新时代改革开放和社会主义现代化建设的实际问题，不断回答（　），作出符合中国实际和时代要求的正确回答，得出符合客观规律的科学认识，形成与时俱进的理论成果，更好指导中国实践。	中国之问	世界之问	人民之问	时代之问

48	多项选择题	党的二十大报告指出，我们必须坚定（　），坚持古为今用、推陈出新，把马克思主义思想精髓同中华优秀传统文化精华贯通起来、同人民群众日用而不觉的共同价值观念融通起来。	道路自信	历史自信	文化自信	制度自信
49	多项选择题	党的二十大报告指出，我们必须增强（　），坚持（　），做到居安思危、未雨绸缪，准备经受风高浪急甚至惊涛骇浪的重大考验。	忧患意识	安全意识	底线意识	底线思维
50	多项选择题	党的二十大报告指出，增强全党全国各族人民的志气、骨气、底气，不信邪、不怕鬼、不怕压，知难而进、迎难而上，统筹（　）和（　），全力战胜前进道路上各种困难和挑战，依靠顽强斗争打开事业发展新天地。	发展	创新	安全	改革
51	多项选择题	“四个意识”是指，政治意识、（　）。	大局意识	忧患意识	核心意识	看齐意识
52	多项选择题	党的二十大报告指出，深入实施（　），优化重大生产力布局，构建优势互补、高质量发展的区域经济布局和国土空间体系。	区域协调发展战略	区域重大战略	主体功能区战略	新型城镇化战略
53	多项选择题	党的二十大报告指出，我们要坚持教育优先发展、科技自立自强、人才引领驱动，加快建设（），坚持为党育人、为国育才，全面提高人才自主培养质量，着力造就拔尖创新人才，聚天下英才而用之。	教育强国	科技强国	人才强国	数字强国
54	多项选择题	“四个伟大”是指，为了实现中华民族伟大复兴，中国共产党团结带领中国人民，自信自强、守正创新，统揽（　）、（　）、伟大事业、（　），创造了新时代中国特色社会主义的伟大成就。	伟大斗争	伟大工程	伟大理想	伟大梦想

55	多项选择题	“三个务必”是指，务必不忘初心、牢记使命；务必谦虚谨慎、（ ）；务必敢于斗争、（ ）。	戒骄戒躁	艰苦奋斗	善于斗争	勇于斗争
56	多项选择题	党的二十大报告指出，我们要健全人民当家作主制度体系，扩大人民有序政治参与，保证人民依法实行（ ）、民主管理、民主监督，发挥人民群众积极性、主动性、创造性，巩固和发展生动活泼、安定团结的政治局面。	民主参政	民主选举	民主协商	民主决策
57	单项选择题	（ ）是我国密码工作最重要、最根本、最核心的原则。	坚持总体国家安全观	坚持中央密码工作领导机构的统一领导	坚持党的领导	坚持集中统一领导
58	单项选择题	（ ）年，中央机构编制委员会批准成立国家密码管理局。	1999	2005	2008	2018
59	单项选择题	2018年，国家密码管理局与（ ），一个机构两块牌子，列入中共中央直属机关的下属机构序列。	中央保密委员会办公室	国家保密局	中央密码工作领导小组办公室	国务院信息化工作办公室
60	单项选择题	关于国家密码管理局的主要职责，下列说法错误的是（ ）。	组织贯彻落实党和国家关于密码工作的方针政策和法律法规	指导密码专业教育和密码学术交流	承办中央保密委员会的部分工作	起草密码工作法规并负责密码法规的解释
61	单项选择题	（ ）年，中央决定在我国大力发展商用密码，加强对商用密码的管理。	1980	1988	1990	1996
62	单项选择题	商用密码检测、认证机构应当依法取得相关资质，下列具有商用密码认证资质的是（ ）。	豪符密码检测技术（成都）有限责任公司	鼎铉商用密码测评技术（深圳）有限公司	智巡密码（上海）检测技术有限公司	以上都没有
63	单项选择题	根据《法律、行政法规、国务院决定设定的行政许可事项清单（2023年版）》，以下（ ）不属于国家密码管理局负责审批的行政许可事项。	商用密码科研成果审查鉴定	商用密码产品质量检测机构资质认定	商用密码科研单位审批	电子政务电子认证服务资质认定

64	单项选择题	党的十八大以来，国务院取消了多项由国家密码管理局负责实施的行政许可事项，目前下列（）还属于行政许可事项。	商用密码产品生产单位审批	商用密码产品销售单位许可	外商投资企业使用境外密码产品审批	商用密码科研成果审查鉴定
65	多项选择题	推进密码应用需要密码管理部门和相关部门密切配合，分工负责，统筹协调，具体应当（　）。	加强顶层制度设计	强调密码管理部门的权力	健全协调工作机制	形成有力的保障机制
66	多项选择题	新时期我国商用密码发展的主要任务包括（　）。	深化商用密码管理改革	强化商用密码专控管理	强化商用密码自主创新	推进商用密码合规正确有效应用
67	多项选择题	数字中国建设“2522”的整体框架是指（　）。	夯实数字基础设施和数据资源体系“两大基础”	推进数字技术与经济、政治、文化、社会、生态文明建设五位一体深度融合	强化数字技术创新体系和数字安全屏障两大能力	优化数字化发展国内国际两个环境
68	多项选择题	《区域全面经济伙伴关系协定》（RCEP）于2022年1月1日正式对中国生效，以下关于RCEP的说法正确的是（　）。	重申密码技术作为主要应用场景的电子签名的法律效力	各缔约国应就网络安全相关的事项开展合作	各缔约国对于计算设施的使用或位置可能有各自的措施，包括寻求保证通信安全和保密的要求	不得将强制要求数据本地化作为其他缔约国在一国领土内进行商业行为的条件
69	多项选择题	根据《国民经济和社会发展第十四个五年规划和2035年远景目标纲要》，以下（　）方面中涉及密码技术和应用。	数据安全	数字货币	数据标准	网络基础设施
70	多项选择题	按照《法律、行政法规、国务院决定设定的行政许可事项清单（2023年版）》，其中涉及密码领域的许可事项包括（　）。	商用密码科研成果审查鉴定	商用密码产品质量检测机构资质认定	电子认证服务使用密码许可	电子政务电子认证服务资质认定
71	多项选择题	根据国家发展改革委、商务部联合发布的《市场准入负面清单（2022 年版）》，以下需国家密码局许可的事项有（　）。	商用密码科研成果审查鉴定	商用密码产品质量检测机构资质认定	电子认证服务许可	电子认证服务使用密码许可
72	判断题	根据《“十四五”推进国家政务信息化规划》，在加强网络安全保障方面包括推进密码应用。	正确	错误		

73	判断题	根据《法律、行政法规、国务院决定设定的行政许可事项清单（2023年版）》，国家密码管理局负责的行政许可事项有四项。	正确	错误		
74	判断题	《“十四五”数字经济发展规划》的五大保障措施明确强化监测评估，其中包括商用密码应用安全性评估。	正确	错误		
75	单项选择题	《密码法》所称密码，是指采用（ ）对信息等进行加密保护、安全认证的技术、产品和服务。	数学变换的方法	移位变换的方法	特定变换的方法	点乘运算的方法
76	单项选择题	《密码法》所称密码，是指采用特定变换的方法对信息等进行（ ）的技术、产品和服务。	加密保护、安全认证	加密保护	安全认证	匿名保护
77	单项选择题	下列哪项不属于《密码法》规范的密码（ ）。	基于格的密码	支付宝登录口令	抗量子密码	税票防伪标识符的加密算法
78	单项选择题	根据《密码法》，密码工作坚持（ ），遵循统一领导、分级负责，创新发展、服务大局，依法管理、保障安全的原则。	总体国家安全观	整体国家安全观	综合国家安全观	安全发展观
79	单项选择题	根据《密码法》，坚持中国共产党对密码工作的领导。（ ）对全国密码工作实行统一领导，制定国家密码工作重大方针政策，统筹协调国家密码重大事项和重要工作，推进国家密码法治建设。	中央国家机关	国家密码管理部门	全国人大常委会	中央密码工作领导机构
80	单项选择题	根据《密码法》，（ ）负责管理全国的密码工作。	国家安全部门	国务院公安部门	国家网信部门	国家密码管理部门
81	单项选择题	根据《密码法》，国家对密码实行（ ）管理。	统一	统筹	分类	有效
82	单项选择题	根据《密码法》，国家对密码实行分类管理，将密码分为（ ）。	核心密码和商用密码	普通密码和商用密码	军用密码和民用密码	核心密码、普通密码和商用密码

83	单项选择题	根据《密码法》，以下哪类密码需要实行严格统一管理（ ）。	核心密码	商用密码产品	商用密码技术	商用密码服务
84	单项选择题	根据《密码法》规定，核心密码、普通密码用于保护国家秘密信息，核心密码保护信息的最高密级为（ ），普通密码保护信息的最高密级为（ ）。	机密级，绝密级	机密级，秘密级	绝密级，机密级	绝密级，秘密级
85	单项选择题	关于《密码法》，下列说法错误的是（ ）。	本法所称的密码并非由数字、字母和符号组成的登录或支付密码	县级以上的人民政府应当将密码工作所需经费列入本级财政预算	采用日常监管和随机抽查相结合的商用密码事中事后监管制度	核心密码、普通密码和商用密码用于保护属于国家秘密的信息
86	单项选择题	根据目前我国法律规范，有关商用密码的说法正确的是（ ）。	互联网企业可以依法使用商用密码保护重要数据	商用密码不能用来保护国家秘密级信息	国家对商用密码实行严格统一管理	国家对商用密码实行分类分级管理
87	单项选择题	依据《密码法》规定，关于商用密码产品的使用，下列说法正确的是（ ）。	我国公民可以依法使用商用密码产品	境外组织在我国境内使用商用密码产品需要报经国家密码管理局批准	我国公民使用商用密码产品需报经国家密码管理局批准	境外个人在我国境内使用商用密码需要报经国家密码管理局批准
88	单项选择题	根据《密码法》，关于商用密码的使用，下列说法错误的是（ ）。	公民可以使用商用密码保护个人信息	关键信息基础设施运营者只能使用商用密码保护国家秘密	重要数据处理者可以使用商用密码保护重要数据	企业可以使用商用密码保护商业秘密
89	单项选择题	根据《密码法》规定，公民、法人和其他组织可以依法使用 （ ）保护网络与信息安全。	核心密码	普通密码	商用密码	民用密码
90	单项选择题	根据《密码法》，国家加强密码（ ）和队伍建设，对在密码工作中作出（ ）的组织和个人，按照国家有关规定给予表彰和奖励。	人才培养，突出贡献	教育培训，突出成绩	人员素质，卓越贡献	教育培训，突出贡献
91	单项选择题	根据《密码法》，国家采取多种形式加强密码安全教育，将密码安全教育纳入（ ），增强公民、法人和其他组织的密码安全意识。	9年义务教育体系和国民教育体系	国民教育体系和公务员教育培训体系	公务员教育体系和成人教育体系	成人教育体系和九年义务教育体系

92	单项选择题	根据《密码法》，县级以上人民政府应当将密码工作纳入本级国民经济和社会发展规划，所需经费列入（　）财政预算。	中央	上级	本级	下级
93	单项选择题	根据《密码法》，任何组织或者个人不得窃取他人加密保护的信息或者非法侵入他人的（　）系统。	加密	密码保障	密码技术	密钥管理
94	单项选择题	根据《密码法》，密码管理部门根据工作需要会同有关部门建立核心密码、普通密码的（　）和应急处置等协作机制，确保核心密码、普通密码安全管理的协同联动和有序高效。	安全监测预警、安全风险评估、信息通报、重大事项会商	安全监测预警、安全风险评估、重大事项会商	安全监测预警、信息共享、重大事项会商	安全风险评估、事件报告、重大事项会商
95	单项选择题	根据《密码法》，密码工作机构发现影响核心密码、普通密码安全的重大问题时，应该（　）。	立即采取措施	及时向保密行政管理部门报告	及时向密码管理部门报告	以上都是
96	单项选择题	根据《密码法》，密码管理部门因工作需要，按照国家有关规定，可以提请有关部门对（　）有关物品和人员提供免检等便利。	商用密码	核心密码、普通密码	核心密码	普通密码
97	单项选择题	根据《密码法》，密码管理部门因工作需要，按照国家有关规定，可以提请（　）等部门对核心密码、普通密码有关物品和人员提供免检等便利，有关部门应当予以协助。	公安	交通运输	海关	以上都对
98	单项选择题	根据《密码法》，密码管理部门和密码工作机构应当建立健全严格的监督和安全审查制度，对其工作人员遵守法律和纪律等情况进行监督，并依法采取必要措施，定期或者不定期组织开展（）。	全方位大检查	安全审查	安全检查	安全评估
99	单项选择题	根据《密码法》，国家鼓励商用密码技术的研究开发、学术交流、成果转化和推广应用，健全（）的商用密码市场体系，鼓励和促进商用密码产业发展。	统一、开放、竞争、有序	和谐、繁荣	稳健高效、开放包容	低风险、高收益

100	单项选择题	根据《密码法》，各级人民政府及其有关部门应当遵循（　），依法平等对待包括外商投资企业在内的商用密码从业单位。	开放原则	平等原则	自愿原则	非歧视原则
101	单项选择题	下列说法不符合《密码法》规定的是（　）。	各级人民政府及其有关部门鼓励和促进商用密码产业发展	依法平等对待包括外商投资企业在内的商用密码从业单位	鼓励在外商投资过程中基于自愿原则和商业规则开展商用密码技术合作	行政机关及其工作人员可利用行政手段强制转让商用密码技术
102	单项选择题	根据《密码法》，国家支持社会团体、企业利用自主创新技术制定（　　）国家标准、行业标准相关技术要求的商用密码团体标准、企业标准。	低于	多于	高于	相当于
103	单项选择题	根据《密码法》，国家鼓励商用密码从业单位采用商用密码（　）、行业标准，提升商用密码的防护能力，维护用户的合法权益。	创新标准	强制性国家标准	国际标准	推荐性国家标准
104	单项选择题	根据《密码法》，国家鼓励商用密码从业单位（）商用密码检测认证，提升市场竞争力。	积极申请	自愿接受	主动申请	被动接受
105	单项选择题	根据《密码法》规定，商用密码检测、认证机构应当依法取得相关资质，并依照法律、行政法规的规定和商用密码检测认证（　）、规则开展商用密码检测认证。	技术规范	最佳实践	实施指南	工作指南
106	单项选择题	根据《密码法》规定，商用密码检测、认证机构应当对其在商用密码检测认证中所知悉的（　）承担保密义务。	国家秘密和商业秘密	国家秘密或商业秘密	国家秘密	商业秘密
107	单项选择题	《密码法》明确了商用密码检测认证制度，下列说法正确的是（　）。	目前我国采用的是商用密码产品品种和型号审批	商用密码服务使用网络关键设备的，实行自愿认证	对涉及社会公共利益的商用密码产品实行自愿性检测制度	在商用密码检测认证中，自愿检测认证成为主要方式

108	单项选择题	根据《密码法》，涉及（　）的商用密码产品，应当依法列入网络关键设备和网络安全专用产品目录，由具备资格的机构检测认证合格后，方可销售或者提供。	国家安全	国计民生	社会公共利益	以上都是
109	单项选择题	根据《密码法》，商用密码服务使用（　）的，应当经商用密码认证机构对该商用密码服务认证合格。	网络关键设备和网络安全专用产品	关键信息基础设施	网络关键设备	网络安全专用产品
110	单项选择题	根据《密码法》，商用密码应用安全性评估应当与（　）、网络安全等级测评制度相衔接，避免重复评估、测评。	关键信息基础设施国家安全审查	网络安全风险评估	关键信息基础设施安全检测评估	网络安全检测、认证
111	单项选择题	根据《密码法》，关键信息基础设施的运营者采购涉及商用密码的网络产品和服务，可能影响国家安全的，应当按照（　）的规定，通过国家网信部门会同国家密码管理部门等有关部门组织的国家安全审查。	《中华人民共和国行政许可法》	《中华人民共和国刑法》	《中华人民共和国网络安全法》	《中华人民共和国安全生产法》
112	单项选择题	《密码法》规定了关键信息基础设施商用密码使用国家安全审查制度，关于这一制度，下列说法正确的是（　）。	该制度是《网络安全法》规定的网络安全审查的一部分	该制度由国家安全部门单独落实	该制度设计初衷主要是维护关键信息基础设施运营者的利益	该制度与《国家安全法》规定的国家安全审查制度是两个独立制度
113	单项选择题	根据《密码法》，商用密码进口许可清单和出口管制清单由国务院商务主管部门会同国家密码管理部门和（　）制定并公布。	市场监管部门	海关总署	国家网信部门	国务院公安部门
114	单项选择题	根据《密码法》，大众消费类产品所采用的商用密码（　）进口许可和出口管制制度。	实行	不实行	选择实行	有条件实行
115	单项选择题	根据《密码法》，实施进口许可的商用密码应符合的条件是（　）。	涉及国家安全且具有安全认证功能	涉及社会公共利益且具有安全认证功能	中国承担国际义务	涉及国家安全、社会公共利益且具有加密保护功能

116	单项选择题	根据《密码法》，关于我国商用密码进口许可和出口管制，下列说法正确的是（ ）。	大众消费类产品所采用的商用密码进出口需要经过许可	商用密码进口许可和出口管制采用清单制	商用密码进出口有白名单制度，列入白名单的国家及地区可以免予许可审批流程	进口许可和出口管制的商用密码范围和类型一致
117	单项选择题	根据《密码法》，国家密码管理部门对采用商用密码技术从事电子政务电子认证服务的机构进行认定，会同有关部门负责政务活动中使用（ ）、数据电文的管理。	电子数据	电子签名	电子文档	电子证照
118	单项选择题	根据《密码法》，关于商用密码领域的行业协会的功能和作用的表述，错误的是（ ）。	为商用密码从业单位提供信息、技术、培训等服务	引导和督促商用密码从业单位依法开展商用密码活动	通过行业自律公约等方式，加强行业自律，推动行业诚信建设	对商用密码从业单位提供检测认证服务
119	单项选择题	《密码法》规定，密码管理部门和有关部门建立统一的商用密码监督管理信息平台，推进事中事后监管与（ ）相衔接。	失信惩戒体系	社会信用体系	国家信用体系	征信体系
120	单项选择题	根据《密码法》，密码管理部门和有关部门建立（ ）的商用密码事中事后监管制度。	定期检查	日常监管和随机抽查相结合	专项行动	双随机、不公开
121	单项选择题	根据《密码法》，发生核心密码、普通密码泄密案件的，由（ ）建议有关国家机关、单位对直接负责的主管人员和其他直接责任人员依法给予处分或者处理。	保密行政管理部门	密码管理部门	保密行政管理部门、密码管理部门	国家安全部门
122	单项选择题	根据《密码法》，商用密码认证机构泄露其在商用密码认证中所知悉的商业秘密，由（ ）会同密码管理部门责令改正或者停止违法行为，给予警告，没收违法所得。	国家网信部门	市场监督管理部门	国务院商务主管部门	海关总署
123	单项选择题	根据《密码法》和《商用密码管理条例》，关于商用密码检测机构违法开展商用密码检测的行政处罚，下列说法正确的是（ ）。	由密码管理部门进行	由市场监督管理部门进行	由市场监督管理部门会同密码管理部门进行	由市场监督管理部门或者密码管理部门进行

124	单项选择题	关键信息基础设施的运营者违反《密码法》规定，使用未经安全审查或者安全审查未通过的产品或者服务，关于应当承担的法律责任，下列错误的是（　）。	由有关主管部门没收违法产品和违法所得	由有关主管部门责令停止使用	由有关主管部门处采购金额一倍以上十倍以下罚款	由有关主管部门对直接负责的主管人员和其他直接责任人员处一万元以上十万元以下罚款
125	单项选择题	《密码法》对关键信息基础设施运营者未按照要求使用商用密码规定的法律责任，下列错误的是（　）。	责令改正	警告	罚款	吊销营业执照
126	单项选择题	根据《密码法》规定，关键信息基础设施的运营者使用未经安全审查或者安全审查未通过的产品或服务，应承担的法律责任包括（　）。	责令停止使用	警告	吊销相关资质	以上都不对
127	单项选择题	违反《密码法》规定进出口商用密码的，由（）依法予以处罚。	国务院商务主管部门会同海关	国务院商务主管部门或者海关	国务院商务主管部门会同密码管理部门	国务院商务主管部门或者密码管理部门
128	单项选择题	根据《密码法》，某单位未经认定从事电子政务电子认证服务，则密码管理部门有权实施的行政处罚包括（）。	警告	没收违法所得	罚款	以上都是
129	单项选择题	《密码法》的正式施行日期是（　）。	2020年1月1日	2021年1月1日	2020年6月1日	2019年10月26日
130	单项选择题	《密码法》规定，我国密码管理体制自上而下分为（　）级。	五	四	三	二
131	单项选择题	（　）不属于《密码法》中规定的国家机关和涉及密码工作的单位。	某市公安局	承担密码管理职责的企业	承担密码管理职责的事业单位	某市密码管理局
132	单项选择题	根据《密码法》，以下关于商用密码检测、认证体系和商用密码检测、认证机构管理的表述，正确的是（　）。	商用密码检测认证中，自愿检测认证是主要方式	商用密码检测认证中，强制检测认证是主要方式	商用密码检测、认证机构资质由国家密码管理局单独管理	商用密码检测、认证机构可以取得统一的商用密码检测认证机构资质

133	单项选择题	根据《密码法》，商用密码认证机构资质纳入《认证认可》条例规定的认证认可制度体系中，由（ ）会同国家密码管理局进行管理。	市场监管总局	公安部	国家互联网信息办公室	工业和信息化部
134	单项选择题	以下哪个产品或服务没有使用商用密码技术（ ）。	网络密码机	第一代居民身份证	密码保障系统集成	社会保障卡
135	单项选择题	根据《密码法》，关于大众消费类产品所采用的商用密码的特点，下列表述正确的是（ ）。	供涉密单位使用	能轻易改变密码功能	通过常规零售渠道购买会受到一定的限制	对国家安全带来的风险较小且可控
136	单项选择题	下列哪一项不属于大众消费类产品所采用的商用密码（ ）。	数字电视智能卡	蓝牙模块	用于知识产权保护的加密狗	有线加密电话机
137	单项选择题	根据《密码法》，国家密码管理部门对采用密码技术从事电子政务电子认证服务的机构进行认定，关于电子政务电子认证服务机构的认定，下列说法正确的是（ ）。	一定程度上与电子认证服务机构存在重复许可	与电子认证服务机构的审批对象一致	可适用于电子商务领域的电子认证服务机构	应当采用行政许可的方式对服务机构的电子政务电子认证服务能力进行评估
138	单项选择题	根据《密码法》，关于电子政务电子认证服务机构认定的审批对象，下列说法正确的是（ ）。	只有经营性企业	不包括提供公共服务的事业单位	只包括提供公共服务的事业单位	包括经营性企业和提供公共服务的事业单位
139	单项选择题	根据《密码法》，在保护涉及（ ）、商业秘密、个人隐私等信息的前提下，密码管理部门和有关部门依法做好商用密码有关信用信息的公开工作。	国家秘密	企业信息	个人信息	情报信息
140	单项选择题	商用密码日常监管实行的“双随机、一公开”方式中，“双随机”指（ ）。	随机抽取检查对象、随机选派执法检查人员	随机抽取密码管理部门、随机选派执法检查人员	随机抽取密码管理部门、随机抽取检查对象	随机抽取检查对象、随机选派检测认证机构
141	单项选择题	商用密码监管中，密码管理部门不得要求商用密码从业单位向其披露密码相关专有信息，以下哪项不属于这类信息（ ）。	源代码	私钥	公钥	算法规范或其他设计细节

142	单项选择题	根据《密码法》，关键信息基础设施运营者未按照要求使用商用密码导致危害网络安全后果的，对直接负责的主管人员处以罚款，下列不属于“直接负责的主管人员”的是（　）。	实施违法行为中起决定作用的人	实施违法行为中起指挥作用的人	授意实施违法行为的人	具体实施违法行为并起较大作用的人
143	单项选择题	关于密码工作表彰奖励，下列说法错误的是（）。	对象主要是在服务党和国家工作大局中发挥重要作用以及在密码科技进步中作出重要贡献的相关组织和个人	坚持精神奖励与物质奖励相结合	以物质奖励为主	表彰奖励工作遵循鼓励创新、促进发展、公平公正、严格把关的原则
144	单项选择题	下列哪个不属于《密码法》规定的关键信息基础设施的运营者违反商用密码使用要求的情形（）。	关键信息基础设施运营者未按照要求使用商用密码	关键信息基础设施运营者未按照要求开展商用密码应用安全性评估	关键信息基础设施运营者使用未经安全审查或者安全审查未通过的产品或服务	关键信息基础设施运营者未按照要求开展商用密码检测认证
145	单项选择题	根据《商用密码知识与政策干部读本》，办理《电子认证服务使用密码许可证》，应首先通过安全性审查，对拟开展电子认证服务的机构建设运营的证书认证系统的（　）进行审查。	功能性能和互联互通情况	功能性能和安全措施	安全措施和互联互通情况	安全措施
146	单项选择题	根据《商用密码应用安全性评估管理办法（试行）》，商用密码应用安全性评估是指对采用商用密码技术、产品和服务集成建设的网络与信息系统密码应用的（　）进行评估。	合规性	正确性	有效性	以上都是
147	单项选择题	根据《商用密码应用安全性评估管理办法（试行）》，关于商用密码应用安全性评估，下列说法错误的是（）。	是对采用商用密码技术、产品和服务集成建设的网络和信息系统使用密码的评估	是对商用密码应用的合规性、正确性、有效性进行评估	涉密的关键信息基础设施应该每半年进行一次商用密码应用安全性评估	基础信息网络应当进行商用密码应用安全性评估

148	单项选择题	根据《商用密码应用安全性评估管理办法（试行）》，下列哪些属于重要领域网络和信息系统（ ）。	基础信息网络	面向社会服务的政务信息系统	重要工业控制系统	以上都是
149	单项选择题	根据《商用密码应用安全性评估管理办法（试行）》，（ ）是商用密码应用安全性评估的责任单位。	涉及国家安全的重要领域网络与信息系统的建设、使用单位	涉及社会公共利益的重要领域网络与信息系统的建设、使用单位	涉及国家安全和社会公共利益的重要领域网络与信息系统的管理单位	以上都是
150	单项选择题	依据《商用密码应用安全性评估管理办法（试行）》规定，商用密码应用安全性评估工作由国家密码管理部门认定的（ ）承担。	密码测评机构	密码认证机构	网络安全服务机构	数据安全检测、评估机构
151	单项选择题	根据《商用密码应用安全性评估管理办法（试行）》，有关商用密码应用安全性评估标准的制定的说法，正确的是（ ）。	国家标准化管理部门单独制定发布商用密码应用安全性评估国家标准	国家密码管理部门制定发布商用密码应用安全性评估国家标准、行业标准	国家标准化管理部门、国家密码管理部门根据各自职责，制定发布商用密码应用安全性评估国家标准、行业标准	国家标准化管理部门会同国家密码管理部门，制定发布商用密码应用安全性评估国家标准、行业标准
152	单项选择题	根据《商用密码应用安全性评估管理办法（试行）》，重要领域网络和信息系统投入运行后，责任单位应当委托测评机构（ ）商用密码应用安全性评估。	于30个工作日内开展	定期开展	不定期开展	于3个工作日内开展
153	单项选择题	根据《商用密码应用安全性评估管理办法（试行）》，有关商用密码应用安全性评估程序的说法，以下错误的是（ ）。	评估工作应遵循独立、客观、公正的原则	责任单位应当在系统规划、建设和运行阶段，组织开展商用密码应用安全性评估工作	测评机构完成商用密码应用安全性评估工作后，应在30个工作日内将评估结果报国家密码管理部门备案	责任单位完成规划、建设、运行和应急评估后，应在30个工作日内将评估结果报国家密码管理部门备案。

154	单项选择题	根据《商用密码应用安全性评估管理办法（试行）》，关于商用密码应用安全性评估程序的表述，以下正确的是（　）。	关键信息基础设施、网络安全等级保护第三级及以上信息系统，每半年至少评估一次	商用密码应用安全性评估未通过，责任单位应当限期整改并重新组织评估	测评机构完成商用密码应用安全性评估工作后，应在15个工作日内将评估结果报国家密码管理部门备案	网络安全等级保护第三级及以上信息系统的责任单位，无需将评估结果报公安部门备案
155	单项选择题	根据《商用密码应用安全性评估管理办法（试行）》，某企业的大数据系统被认定为网络安全等级保护第三级，则该单位的商用密码应用安全性评估结果除了上报所在地区密码管理部门备案，还应同时报所在地区（　）备案。	人民政府	网信部门	工信部门	公安部门
156	单项选择题	根据《商用密码应用安全性评估管理办法（试行）》，国家密码管理部门根据工作需要，（）对各地区（部门）商用密码应用安全性评估工作开展检查。	定期	不定期	每年	每半年
157	单项选择题	根据《商用密码应用安全性评估管理办法（试行）》，国家密码管理部门对测评机构进行监督检查，并根据需要对测评机构的评估结果进行（）。	定期检查	专项检查	不定期检查	抽查
158	单项选择题	根据《商用密码应用安全性测评机构管理办法（试行）》，下列哪个企业可能具备申请商用密码应用安全性测评机构的基本条件（　）。	某事业单位具有专业技术人员和管理人员，通过“商用密码应用安全性测评人员考核”的测评人员数量共8人	某科技公司产权关系明晰，注册资金600万元	某科技公司成立2年，从事信息系统安全相关工作半年，无违法记录	某事业单位具备与从事系统测评相适应的独立、集中、可控的工作环境，测评工作场地150平方米

159	单项选择题	根据《商用密码应用安全性测评机构管理办法（试行）》，对申请成为商用密码应用安全性测评机构的单位在注册资金方面的要求，下列说法正确的是（　）。	注册资金200万元以上	注册资金500万元以上	注册资金800万元以上	注册资金1000万元以上
160	单项选择题	根据《商用密码应用安全性测评机构管理办法（试行）》，申请成为商用密码应用安全性测评机构的单位在测评工作场地方面有要求，下列说法正确的是（　）。	应不少于50平方米	应不少于100平方米	应不少于200平方米	应不少于300平方米
161	单项选择题	根据《商用密码应用安全性测评机构管理办法（试行）》，对申请成为商用密码应用安全性测评机构的单位在成立年限方面的要求，下列说法正确的是（　）。	成立年限在1年以上，从事信息系统安全相关工作1年以上	成立年限在2年以上，从事信息系统安全相关工作1年以上	成立年限在2年以上，从事信息系统安全相关工作半年以上	成立年限在3年以上，从事信息系统安全相关工作1年以上
162	单项选择题	根据《商用密码应用安全性测评机构管理办法（试行）》，对申请成为商用密码应用安全性测评机构的单位在测评人员方面的要求，下列说法正确的是（　）。	具有本科以上学历和密码相关经验	测评人员的审核以通过培训的测评人员名单为依据	测评人员可以为申请单位的第三方长期外包人员	具有硕士以上学历和密码相关经验
163	单项选择题	根据《商用密码应用安全性评估管理办法（试行）》，对申请成为商用密码应用安全性测评机构的单位在测评技术负责人方面的要求，下列说法正确的是（　）。	从事商用密码或质量管理相关工作5年以上	从事商用密码或质量管理相关工作3年以上	从事商用密码或质量管理相关工作2年以上	从事商用密码或质量管理相关工作1年以上
164	单项选择题	根据《商用密码应用安全性测评机构管理办法（试行）》，对申请成为商用密码应用安全性测评机构的单位在测评人员方面的要求，下列说法正确的是（　）。	配备测评技术负责人1名，不需要质量负责人	配备质量负责人1名，不需要测评技术负责人	配备测评技术负责人与质量负责人各1人	配备测评技术负责人与质量负责人各2人

165	单项选择题	根据《商用密码应用安全性测评机构管理办法（试行）》，申请成为商用密码应用安全性测评机构的单位，有校准要求的仪器设备需按时送至校准实验室进行专门校准，并确保所进行的校准可溯源到（　）。	公制	国际单位制	米制	英制
166	单项选择题	根据《商用密码应用安全性测评机构管理办法（试行）》，国家密码管理部门会同（　）制定测评机构的有关技术与管理规范，组织测评机构业务培训。	国务院公安部门	国务院电信主管部门	国家网信部门	国家密码管理部门
167	单项选择题	根据《商用密码应用安全性测评机构管理办法（试行）》，重要领域网络和信息系统规划阶段，（　）应当依据商用密码应用安全性有关标准，制定商用密码应用建设方案。	运营单位	责任单位	技术支撑单位	建设单位
168	单项选择题	根据《商用密码应用安全性测评机构管理办法（试行）》，申请成为商用密码应用安全性测评机构的单位应当提交的材料不包括（　）。	从事与普通密码相关工作情况的说明	开展测评工作所需的软硬件及其他服务保障设施配备情况	管理制度建设情况	《商用密码应用安全性测评机构申请表》
169	单项选择题	根据《商用密码应用安全性测评机构管理办法（试行）》，通过国家密码管理局初审的商用密码应用安全性测评机构申请单位，应在（　）工作日内参加培训、考核和能力评审。	30个	45个	60个	90个
170	单项选择题	根据《商用密码应用安全性测评机构管理办法（试行）》，（　）的商用密码应用安全性评估结果应作为项目建设验收的必备材料。	重要领域网络和信息系统建设完成后	涉及绝密级的电子政务系统	涉及秘密级的国家政务系统	涉及机密级的电子政务系统

171	单项选择题	根据《商用密码应用安全性测评机构管理办法（试行）》，商用密码应用安全性测评机构的下列哪项发生变更的，可以不用向国家密码管理局报告（　）。	甲测评机构的名称从xx信息科技有限公司修改为xxx科技有限公司	乙测评机构法人由王某变更为李某	丙测评机构股东因重病将本单位股份转让给其他股东	丁测评机构因改革裁员辞退技术人员5人，使得原本20人的技术团队变为15人
172	单项选择题	根据《商用密码应用安全性测评机构管理办法（试行）》，关于密码管理机构对商用密码应用安全性测评机构开展的监督检查活动，下列符合法律规范要求的是（　）。	F市密码管理局对E市的测评机构开展监督检查	E省密码管理局对C省的测评机构开展监督检查	D省密码管理局对D省的测评机构开展监督检查	E市密码管理局对E市的测评机构开展监督检查
173	单项选择题	根据《商用密码应用安全性测评机构管理办法（试行）》，商用密码应用安全性测评机构测评人员培训、考核工作由（　）承担。	商用密码应用安全性测评机构自己	国家密码管理局	国家密码管理局遴选的专门专家组	国家密码管理局委托的机构
174	单项选择题	根据《商用密码应用安全性测评机构管理办法（试行）》，商用密码应用安全性测评机构应当（　）编制商用密码应用安全性评估工作报告，并报送国家密码管理局。	在年底	于1月31日之前	于6月30日之前	于9月30日之前
175	单项选择题	根据《商用密码应用安全性测评机构管理办法（试行）》，符合下列哪项情形的，国家密码管理局应取消其商用密码应用安全性测评机构试点资格（　）。	测评机构在一次测评行为中出现失误，对测评结果产生影响	测评机构故意泄露被测评单位工作秘密	测评机构出具测评报告忘记盖章	以上都不对
176	单项选择题	根据《商用密码应用安全性测评机构能力评审实施细则（试行）》，国家密码管理局成立由（）专家组成的评审专家组，组织商用密码应用安全性测评机构能力的专家评审。	2名	3-5名	5-7名	10名以上
177	单项选择题	根据《关于开展商用密码检测认证工作的实施意见》，商用密码认证目录由（　）发布。	市场监管总局	国家密码管理局	市场监管总局、国家密码管理局共同	以上都不对

178	单项选择题	根据《关于开展商用密码检测认证工作的实施意见》，市场监管总局、国家密码管理局联合组建（　），协调解决认证实施过程中出现的技术问题，为管理部门提供技术支撑、提出工作建议等。	商用密码认证监督委员会	商用密码认证技术委员会	专门机构	商用密码认证协调委员会
179	单项选择题	《关于开展商用密码检测认证工作的实施意见》的制定依据不包括（　）。	《中华人民共和国产品质量法》	《中华人民共和国密码法》	《中华人民共和国认证认可条例》	《中华人民共和国商用密码管理条例》
180	单项选择题	根据《关于开展商用密码检测认证工作的实施意见》，下列有关商用密码检测、认证机构的说法，错误的是（　）。	商用密码认证机构应当委托依法取得商用密码检测相关资质的检测机构开展与认证相关的检测活动	商用密码检测、认证机构应当按照有关规定报送商用密码检测、认证实施情况及检测、认证证书信息	商用密码检测、认证机构应当对其在商用密码检测认证中所知悉的国家秘密和商业秘密承担保密义务	商用密码检测、认证机构应当对其在商用密码检测认证中所知悉的国家秘密和商业秘密承担保密义务
181	单项选择题	《商用密码管理条例》的颁布时间是（　）。	2023年4月27日	2023年5月27日	1999年10月7日	1999年11月7日
182	单项选择题	为了贯彻落实《密码法》，国家密码管理局起草了《商用密码管理条例（修订草案征求意见稿）》，征求意见的时间开始于（　）。	2017年8月20日	2020年8月20日	2021年8月20日	2022年8月20日
183	单项选择题	《商用密码管理条例》修订的考虑因素不包括（　）。	党的十八大以来，党中央、国务院对商用密码创新发展和行政审批制度改革提出了系列要求	2019 年发布的《密码法》对商用密码管理制度进行了结构性重塑	1996年，中央决定在我国大力发展商用密码，加强对商用密码的管理	适应新时代商用密码事业发展需求，依法解决商用密码技术进步和商用密码事业发展中出现的新情况新问题
184	单项选择题	2017年12月，国家密码管理局公布《国家密码管理局关于废止和修改部分管理规定的决定》，其中废止的管理规定不包括（　）。	《商用密码产品销售管理规定》	《商用密码产品使用管理规定》	《境外组织和个人在华使用密码产品管理办法》	《商用密码科研管理规定》

185	单项选择题	根据《电子认证服务密码管理办法》，采用密码技术为社会公众提供第三方电子认证服务的系统使用（　）。	核心密码	普通密码	商用密码	核心密码和普通密码
186	单项选择题	根据《电子认证服务密码管理办法》，申请《电子认证服务使用密码许可证》的材料由省、自治区、直辖市密码管理机构受理的，应当自受理申请之日起（　）将全部申请材料报送国家密码管理局。	5个工作日内	10个工作日内	20个工作日内	30个工作日内
187	单项选择题	根据《电子认证服务密码管理办法》，国家密码管理局应当对《电子认证服务使用密码许可证》申请人提交的申请材料进行审查，组织对电子认证服务系统进行（　）。	安全性审查或互联互通测试	安全性审查和互联互通测试	技术性审查和互联互通测试	技术性审查或互联互通测试
188	单项选择题	根据《电子认证服务密码管理办法》，电子认证服务提供者变更名称的，应当自变更之日起（），持变更证明文件到所在地的省、自治区、直辖市密码管理机构办理《电子认证服务使用密码许可证》更换手续。	10日内	20日内	30日内	45日内
189	单项选择题	根据《电子认证服务密码管理办法》，对电子认证服务提供者使用密码情况进行监督检查的方式，下列说法正确的是（　）。	书面审查和现场核查相结合	只能书面审查	只能现场核查	远程检查
190	单项选择题	根据《关于发布商用密码进口许可清单、出口管制清单和相关管理措施的公告》，商用密码进口许可清单、出口管制清单制定的法律依据不包括（　）。	《中华人民共和国密码法》	《中华人民共和国出口管制法》	《中华人民共和国海关法》	《中华人民共和国保守国家秘密法》

191	单项选择题	根据《关于发布商用密码进口许可清单、出口管制清单和相关管理措施的公告》，我国实行出口管制的加密VPN设备以IPSec/SSL VPN为主要功能的设备，其特征之一是加密通信速率（　）以上。	10Gbps	20Gbps	50Gbps	100Gbps
192	单项选择题	根据《关于发布商用密码进口许可清单、出口管制清单和相关管理措施的公告》，我国实行出口管制的密钥管理产品是用于对称密钥或非对称密钥的生成、分发、存储等管理功能的服务端设备，其特征之一是支持管理对象数量（　）以上。	5000	10000	15000	20000
193	单项选择题	根据《关于发布商用密码进口许可清单、出口管制清单和相关管理措施的公告》，我国对采用密码技术实现数据传输加密保护等功能，含有（）密钥长度基于椭圆曲线的非对称密码算法的传真机实行进口许可。	32位以上	64位以上	128位以上	768位以上
194	单项选择题	根据《关于发布商用密码进口许可清单、出口管制清单和相关管理措施的公告》，商务部应当自收到商用密码进出口许可申请文件之日起会同（）等有关部门进行审查。	国家密码管理局	海关	国家互联网信息办公室	国家保密局
195	单项选择题	根据《关于发布商用密码进口许可清单、出口管制清单和相关管理措施的公告》，申请经审查予以许可的，由（　）颁发两用物项和技术进出口许可证。	商务部	海关	国家密码管理局	公安部

196	单项选择题	根据《关于发布商用密码进口许可清单、出口管制清单和相关管理措施的公告》，（ ）应当自收到两用物项和技术进出口申请表及相关文件之日起会同国家密码管理局等有关部门进行审查，并在法定期限内作出许可或者不予许可的决定。	商务部	海关总署	市场监管总局	国家互联网信息办公室
197	单项选择题	我国《商用密码管理条例》特别重视商用密码科技创新工作，根据相关规定，下列选项中表述正确的是（ ）。	商用密码不可以通过知识产权进行保护	外商投资过程中应当基于行政要求，而非商业规则开展商用密码技术合作	商用密码科学技术成果属于国家秘密，不得发布	行政机关及其工作人员不得利用行政手段强制转让商用密码技术
198	单项选择题	根据《商用密码管理条例》规定，关于商用密码标准化，下列选项中表述正确的是（ ）。	商用密码中国标准不能与国外标准转化	国家密码管理部门独立负责制定商用密码国家标准	国家密码管理部门应当对商用密码标准的实施进行监督检查	为促进商用密码技术发展，其他领域的标准如果涉及商用密码，可以不与商用密码行业标准保持协调
199	单项选择题	根据《商用密码管理条例》规定，关于商用密码检测认证，下列选项中表述正确的是（ ）。	商用密码涉及网络安全，商用密码活动必须接受商用密码检测认证	通过商用密码检测认证后，从事商用密码相关活动将不再需要许可	商用密码检测认证机构应当经国家密码管理部门认定	商用密码检测认证机构应当取得相应资质
200	单项选择题	根据《商用密码管理条例》规定，取得商用密码认证机构资质，应当符合相应程序，下列选项中表述正确的是（ ）。	应当向国家密码管理部门提出书面申请	国家密码管理部门审查资质申请时，应当征求国务院市场监督管理部门意见	应当向国务院市场监督管理部门提出书面申请	国务院市场监督管理部门应当独立审查资质申请
201	单项选择题	根据《商用密码管理条例》规定，甲公司提供商用密码服务的过程中，使用到被列入网络关键设备和网络安全专用产品目录的商用密码产品，下列选项中表述正确的是（ ）。	该商用密码产品应当检测认证合格	商用密码服务本身不需要认证合格	可以选择对该商用密码产品进行检测认证或对密码服务本身进行认证	不需要进行任何形式的检测认证

202	单项选择题	根据《商用密码管理条例》规定，甲公司系外商独资企业，欲在我国开展电子政务电子认证服务，下列选项中表述正确的是（ ）。	甲公司在我国不能从事电子政务电子认证服务	可以对甲公司进行外商投资安全审查	甲公司应当向国务院市场监督管理部门提出申请	电子政务电子认证服务同样属于电子认证服务，甲公司无需经过主管部门认定
203	单项选择题	根据《商用密码管理条例》规定，某市高新区行政审批局为提升服务效率并保障数据安全，在审批流程中开始大量使用电子签名，针对电子签名的管理，下列选项中表述正确的是（ ）。	密码管理部门无权对该电子签名进行管理	行政审批局应当使用由密码管理部门提供的电子签名	行政审批局应当使用由依法设立的电子政务电子认证服务机构提供的电子签名	行政审批局可以使用任何电子签名
204	单项选择题	根据《商用密码管理条例》规定，甲公司欲进口境外商用密码技术用于其自主研发的产品中，下列选项中表述正确的是（ ）。	甲公司在任何情况下均需要取得进口许可	即便境外商用密码技术仅具备认证功能，甲公司也需要取得进口许可	只有在境外商用密码技术被列入商用密码进口许可清单，甲公司才需要取得进口许可	甲公司的产品即使属于大众消费类产品，也需要取得进口许可
205	单项选择题	根据《商用密码管理条例》规定，甲公司系我国一家商用密码科研机构，其获得出口许可后，向A国乙公司出售一款商用密码产品。乙公司在使用后认为该款商用密码产品功能强大，欲出售给B国的关联公司丙公司使用，下列选项中表述正确的是（ ）。	甲公司已经依法取得出口许可，故乙公司可以自由出售给丙公司	乙公司向丙公司出售，仍然应当获得我国的出口许可证	乙公司向丙公司出售是否需要获得出口许可，应当以A国法律规定为准	即使甲公司的商用密码产品属于大众消费类产品，也需要获得我国的出口许可证
206	单项选择题	根据《商用密码管理条例》规定，甲公司进口某款境外商用密码产品，但并未向海关交验进口许可证。海关在查验过程中，认为甲公司进口的商用密码产品应当属于我国商用密码进口许可清单的范围，应当申领商用密码进口许可证。下列选项中表述正确的是（ ）。	无论甲公司是否认可，海关均应当当场予以收缴	海关可以向国家密码管理部门提出组织鉴别	海关应当首先向甲公司提出质疑	在鉴别或者质疑期间，由于并不能认定甲公司违反商用密码进出口管理规定，海关应当首先对甲公司进口的产品予以放行

207	单项选择题	根据《商用密码管理条例》规定，关键信息基础设施只有通过商用密码应用安全性评估方可投入使用，并且在运行后仍然需要进行评估。下列选项中表述正确的是（ ）。	运行后每半年至少评估一次	运行后每年至少评估一次	运行后每年至少评估二次	运行后每二年至少评估一次
208	单项选择题	根据《商用密码管理条例》规定，关于密码管理部门和有关部门开展商用密码监督检查，下列选项中表述正确的是（ ）。	查封商用密码活动场所	要求违法单位披露源代码	冻结涉案账户	查阅、复制有关合同、票据、账簿以及其他有关资料
209	单项选择题	根据《商用密码管理条例》规定，某商用密码检测机构为扩展业务影响，其通过出具虚假检测数据和结果的方法吸引客户，违法所得25万元，密码管理部门拟对其进行处罚，下列选项中表述正确的是（ ）。	在没收违法所得同时，可以并处违法所得1倍以上3倍以下罚款	在没收违法所得同时，可以并处10万元以上30万元以下罚款	在没收违法所得外不能再处以罚款	可以禁止该商用密码检测机构负责人在一定时期内不得再从事相关职业
210	单项选择题	根据《商用密码管理条例》规定，某市政府在使用某电子政务电子认证服务机构提供的电子签名过程中，出现电子签名失效的情况，导致相关政务信息产生泄露风险下列选项中表述正确的是（ ）。	市政府需要证明电子签名存在瑕疵，方可获得赔偿	市政府无需任何证明，就可获得赔偿	电子政务电子认证机构需要证明自己无过错，否则就需要进行赔偿	即使该电子签名存在瑕疵，但只要电子政务电子认证机构证明市政府同样存在操作不当，就可以免于赔偿
211	单项选择题	根据《商用密码管理条例》规定，某关键信息基础设施运营者明知其采购的商用密码产品未通过网络安全审查，但出于成本考虑，仍然继续使用，下列选项中表述正确的是（ ）。	应当处1万元以上10万元以下罚款	应当处采购金额1倍以上10倍以下罚款	不可以对主管人员处以罚款	有关主管部门无权直接责令停止使用该商用密码产品
212	多项选择题	根据《密码法》，关于密码分类的说法正确的是（ ）。	密码分为核心密码、普通密码和商用密码	核心密码、普通密码和商用密码都是采用特定变换的方法对信息等进行加密保护、安全认证	核心密码和商用密码属于一类	普通密码和商用密码属于一类

213	多项选择题	以下关于《密码法》的说法正确的有（　　）。	《密码法》规范的是密码应用和管理	密码工作应坚持总体国家安全观	密码工作坚持中国共产党的领导	国家密码管理部门负责管理密码工作
214	多项选择题	根据《密码法》，有关核心密码、普通密码和商用密码说法正确的是（　　）。	核心密码、普通密码用于保护国家秘密信息	核心密码、普通密码属于国家秘密	商用密码可以用于在互联网中保护信息	商用密码用于保护不属于国家秘密的信息
215	多项选择题	根据《密码法》，密码工作坚持党的绝对领导体现在以下哪些方面（　　）。	密码工作的重大事项向中央报告	密码工作的重大决策由中央决定	坚决贯彻执行中央关于密码工作的方针政策，落实中央确定的密码工作领导和管理体制	充分发挥党的领导核心作用，各级党委(党组)和密码工作领导机构要认真履行党管密码的政治责任
216	多项选择题	《密码法》是密码领域的综合性、基础性法律，制定该法的目的包括（　　）。	规范密码应用和管理	促进密码事业发展	保障网络与信息安全	维护国家安全和社会公共利益
217	多项选择题	根据《密码法》，对密码定义中加密保护、安全认证的理解正确的有（　　）。	密码可用于实现加密保护的功能	密码可用于实现安全认证的功能	国务院商务主管部门、国家密码管理部门依法对涉及国家安全、社会公共利益且具有加密保护功能的商用密码实施进口许可	国务院商务主管部门、国家密码管理部门依法对涉及国家安全、社会公共利益且具有安全认证功能的商用密码实施进口许可
218	多项选择题	根据《密码法》，密码工作应坚持的原则包括（）。	依法管理	统一负责	服务大局	创新发展
219	多项选择题	根据《密码法》，下列关于我国密码工作管理体制的表述，正确的有（　）。	国家密码管理部门负责管理全国的密码工作	县级以上地方各级密码管理部门负责管理本行政区域的密码工作	国家机关和涉及密码工作的单位在其职责范围内负责本机关、本单位或者本系统的密码工作	密码工作保护部门负责本行业、本领域的密码工作

220	多项选择题	根据《密码法》，商用密码可用于保护的信息有（ ）。	绝密级信息	商业秘密信息	个人隐私信息	非国家秘密的工作秘密信息
221	多项选择题	下列属于《密码法》禁止的密码违法犯罪行为有（ ）。	贾某未经授权访问其用户的密码保障系统	李某为寻找出轨证据，拦截其女友的加密通信信息	张某私自加密了室友的毕业论文，并匿名索要解密赎金	季某为褚某实施的加密勒索行为提供支付结算业务
222	多项选择题	根据《密码法》，商用密码领域的行业协会的功能和作用包括（ ）。	为商用密码从业单位提供信息、技术、培训等服务	引导和督促商用密码从业单位依法开展商用密码活动	通过行业自律公约等方式，加强行业自律，推动行业诚信建设	对商用密码从业单位开展收费检测认证
223	多项选择题	根据《密码法》，密码管理部门的事中事后监管制度包括哪些内容（ ）。	建立统一的商用密码监督管理信息平台，向社会发布监管信息	开展各类日常监管活动	开展随机抽查活动	将监管信息与社会信用体系相衔接
224	多项选择题	根据《密码法》，国家密码管理部门的机构设置不正确的是（ ）。	国家、省级两级	国家、省级与设区的市级三级	国家、省级、设区的市级和县级四级	国家、省级、设区的市级、县级和乡镇级五级
225	多项选择题	根据《密码法》，我国商用密码市场体系建设的目标包括（ ）。	统一	开放	竞争	有序
226	多项选择题	根据《密码法》，以下属于商用密码从业单位的有（ ）。	某外商投资商用密码研发企业	某国有商用密码生产企业	某自然人控股的商用密码服务企业	某混合所有制的商用密码销售企业
227	多项选择题	根据《密码法》，我国对于外商投资商用密码企业应当秉承的态度包括（ ）。	各级人民政府及其有关部门应当遵循非歧视原则	依法平等对待包括外商投资企业在内的商用密码科研、生产、销售、服务、进出口等单位	鼓励在外商投资过程中基于自愿原则和商业规则开展商用密码技术合作	行政机关及其工作人员不得利用行政手段强制外商投资商用密码企业转让商用密码技术
228	多项选择题	我国积极推动参与商用密码国际标准化活动，根据《密码法》，以下可以参与制定商用密码国际标准的主体有（ ）。	企业	社会团体	教育机构	科研机构

229	多项选择题	根据《密码法》的规定，国家鼓励商用密码从业单位提升商用密码的防护能力，维护用户的合法权益，采用的标准有（ ）。	推荐性国家标准	行业标准	团体标准	企业标准
230	多项选择题	根据《密码法》，下列违反了商用密码产品、服务市场准入制度的情形有（ ）。	销售列入网络关键设备和网络安全专用产品目录的商用密码产品，未经具备资格的机构检测认证	提供列入网络关键设备和网络安全专用产品目录的商用密码产品，检测认证不合格	提供使用网络关键设备和网络安全专用产品的商用密码服务,未经商用密码认证机构认证	提供使用网络关键设备和网络安全专用产品的商用密码服务,认证不合格
231	多项选择题	根据《密码法》，应当依法列入网络关键设备和网络安全专用产品目录的商用密码产品有（ ）。	涉及国家安全	涉及国计民生	涉及社会公共利益	涉及个人隐私
232	多项选择题	根据《密码法》，某科研单位依据国家有关规定列入需要使用商用密码进行保护的关键信息基础设施，下列正确的表述有（ ）。	该科研单位可以不使用商用密码进行保护，但需要向主管部门说明理由	该科研单位可以自行开展商用密码应用安全性评估	该科研单位可以委托商用密码检测机构开展商用密码应用安全性评估	该科研单位出于保密考虑，有权拒绝实施商用密码应用安全性评估
233	多项选择题	根据《密码法》，我国商用密码出口管制的适用对象包括（ ）。	涉及国家安全的	涉及社会公共利益的	涉及大众消费的	涉及中国承担国际义务的
234	多项选择题	《密码法》规定商用密码进出口监管清单包括（ ）。	《商用密码进口许可清单》	《商用密码出口管制清单》	《商用密码进口审查清单》	《商用密码进出口监管目录》
235	多项选择题	商用密码认证机构应当依法取得相关资质，根据《认证认可条例》《商用密码管理条例》，其应当满足的条件包括（ ）。	有固定的场所和必要的设施	有符合认证认可要求的管理制度	有10名以上相应领域的专职认证人员	具备与从事商用密码认证活动相适应的检测、检查等技术能力
236	多项选择题	根据《密码法》，密码管理部门和有关部门建立商用密码事中事后监管制度，并推进事中事后监管与社会信用体系相衔接，从而强化商用密码从业单位自律和社会监督。其中，事中事后监管制度包括（ ）。	行政许可	事后审查	日常监管	随机抽查

237	多项选择题	根据《密码法》，以下属于商用密码从业单位的有商用密码（　）单位。	科研	生产、销售	服务	进出口
238	多项选择题	根据《密码法》，以下符合商用密码的非歧视原则的做法包括（　）。	依法平等对待包括外商投资企业在内的商用密码从业单位	基于自愿原则和商业规则开展商用密码技术合作	不得利用行政手段强制转让商用密码技术	利用行政手段强制转让商用密码技术
239	多项选择题	根据《密码法》，国家密码管理部门依据职责制定的商用密码标准不属于（　）。	国家标准	行业标准	团体标准	企业标准
240	多项选择题	根据《密码法》，以下关于商用密码企业标准的说法正确的是（　）。	企业标准是企业利用自主创新技术制定的标准	企业标准应不低于强制性国家标准的相关技术要求	企业执行自行制定的企业标准的，企业标准对其具有约束力	企业标准可以直接上升为国家标准
241	多项选择题	根据《密码法》，以下关于商用密码国家标准的说法正确的是（　）。	分为强制性标准、推荐性标准	目前尚无商用密码的强制性国家标准	企业标准应高于国家标准、行业标准相关技术要求	强制性国家标准必须执行
242	多项选择题	根据《密码法》，以下关于商用密码国际标准的说法正确的是（　）。	国家推动参与商用密码国际标准化活动	国外的密码标准可以直接适用于国内	国家可以结合国情采用国际标准	企业可以参与国际标准化活动
243	多项选择题	根据《密码法》，商用密码标准体系包括（　）。	国家标准	团体标准	个人标准	行业标准
244	多项选择题	根据《密码法》，以下关于网络关键设备和网络安全专用产品目录说法正确的是（　）。	目录是基于《网络安全法》第23条确立的管理制度	依据《密码法》和《网络安全法》分别建立不同的目录	目录按照需求分批次发布	《网络关键设备安全通用要求》是强制性国家标准

245	多项选择题	根据《密码法》，关于列入网络关键设备和网络安全专用产品目录的商用密码产品，以下说法正确的是（　）。	一般是涉及国家安全、国计民生、社会公共利益和敏感个人信息的产品	应由具备资格的机构检测认证合格后方可销售或者提供	商用密码服务使用目录产品的，还需要经商用密码服务认证合格	《网络关键设备安全通用要求》和《网络关键设备和网络安全专用产品安全认证实施规则》等提供了检测认证的具体要求
246	多项选择题	根据《密码法》，关于在有线、无线通信中传递的国家秘密信息，以及存储、处理国家秘密信息的信息系统，以下说法不正确的是（　）。	应按照法律法规和规定使用核心密码、普通密码	必要时可以使用商用密码进行临时传递和存储	使用AES 256进行加密保护	通过采购公有云和部署密码技术以提升集约化和安全水平
247	多项选择题	根据《密码法》，以下属于核心密码和普通密码工作机构的密码活动的有（　）。	密码科研	密码生产、服务	密码进出口	密码使用、销毁
248	多项选择题	根据《密码法》，从事核心密码、普通密码的密码工作机构，需（　），确保核心密码、普通密码的安全。	建立健全安全管理制度	采取严格的保密措施	形成可考核、可评价的保密责任制	采购列入网络关键设备和网络安全专用产品目录的商用密码产品
249	多项选择题	根据《密码法》，（　）不属于依法对密码工作机构的核心密码、普通密码工作进行指导、监督和检查的主体。	国家保密部门	密码管理部门	国家市场监督管理部门	国家民政部门
250	多项选择题	《密码法》明确的核心密码、普通密码泄密案件或者密码工作机构违反相关安全要求的具体情形包括（　）。	发生核心密码、普通密码泄密案件	发现核心密码、普通密码泄密或者影响核心密码、普通密码安全的重大问题、风险隐患,未立即采取应对措施。	发现核心密码、普通密码泄密或者影响核心密码、普通密码安全的重大问题、风险隐患,未立即向社会发布预警通告	发现核心密码、普通密码泄密或者影响核心密码、普通密码安全的重大问题、风险隐患,未及时向保密行政管理部门、密码管理部门报告

251	多项选择题	根据《密码法》，核心密码、普通密码安全的跨部门协作保障机制包括（　）。	安全监测预警	安全风险评估	信息通报	重大事项会商和应急处置
252	多项选择题	根据《密码法》，密码管理部门如因工作需要寻求核心密码、普通密码有关物品和人员免检便利的，可以向（　）提请协助。	海关	交通运输	公安	工商管理局
253	多项选择题	根据《密码法》，保护密码科学技术研究和应用的知识产权机制有（　）。	专利	著作权	工业产权	商标
254	多项选择题	国家采取多种形式加强密码安全教育，根据《密码法》，以下包括了密码安全教育内容的教育体系有（　）。	义务教育	公务员教育培训	高等教育	职业教育
255	多项选择题	根据《密码法》，关于商用密码行业协会的说法，正确的是（　）。	目前很多省（自治区、直辖市）已经设立了商用密码行业协会	行业协会需经民政部门登记成立，否则属于非法组织	商用密码行业协会有助于实现密码行业的规范、健康发展	企业可以自愿申请加入行业协会
256	多项选择题	根据《密码法》《商用密码应用安全性评估管理办法（试行）》，以下关于商用密码应用安全性评估的说法正确的是（　）。	密码保障网络安全的核心支撑作用需要通过应用安全性评估实现	涉及国家安全和社会公共利益的重要领域网络和信息系统需要进行商用密码应用安全性评估	商用密码应用安全性评估是对密码应用的合规性、正确性和有效性进行的评估	《网络安全法》首次明确提出了商用密码应用安全性评估
257	多项选择题	根据《密码法》，以下需要进行商用密码应用安全性评估的情况有（　）。	重要领域网络和信息系统建成后	重要领域网络和信息系统运行后的定期（不少于每年一次）	重要领域网络和信息系统发生密码相关重要事件	重要领域网络和信息系统发生密码应用重大变化
258	多项选择题	根据《商用密码应用安全性评估管理办法（试行）》，网络安全等级保护三级以上信息系统的责任单位在完成商用密码应用安全性评估后，应向哪些部门履行备案手续（　）。	主管部门	所在地区密码管理部门	所在地区发改部门	所在地区公安部门

259	多项选择题	根据《商用密码应用安全性测评机构管理办法（试行）》，关于商用密码应用安全性测评机构，以下说法正确的是（　）。	测评机构应经国家密码管理部门认定	测评机构目录由国家密码管理部门发布	测评机构应按照商用密码相关标准开展具体测评工作	测评机构应符合《认证认可条例》等规定的资质条件
260	多项选择题	根据《密码法》，对采用商用密码技术从事电子政务电子认证服务的机构，以下说法正确的是（）。	国家密码管理部门应对采用商用密码技术从事电子政务电子认证服务的机构进行认定	采用商用密码技术从事电子政务电子认证服务属于电子认证服务	采用商用密码技术从事电子政务电子认证服务不属于电子认证服务	未经认定从事电子政务电子认证服务的，将承担没收违法产品和违法所得，并处罚款等的法律责任
261	多项选择题	根据《密码法》，关于商用密码检测认证体系建设的说法正确的有（　）。	商用密码从业单位基于自愿原则接受商用密码检测认证，另有规定的除外	商用密码检测、认证机构应当依法取得相关资质	商用密码检测认证体系参与主体包括商用密码检测、认证机构和商用密码产业单位	商用密码检测、认证机构应向密码管理部门披露密码源代码
262	多项选择题	根据《密码法》，商用密码检测认证工作的监管机构有（　）。	国家密码管理局	国家保密局	市场监管总局	工商管理局
263	多项选择题	按照《密码法》，商用密码检测认证工作的监管机构主要负责对哪些市场主体的监管（　）。	商用密码认证机构	取得商用密码检测相关资质的检测机构	未取得商用密码检测相关资质的检测机构	商用密码进出口单位
264	多项选择题	根据《密码法》，以下属于商用密码检测认证的法律依据的是（　）。	《密码法》	《认证认可条例》	《产品质量法》	《标准化法》
265	多项选择题	以下哪些不符合《密码法》的商用密码检测认证规定（　）。	检测认证仅涉及密码技术、产品或服务的安全认证功能	商用密码生产、销售单位应强制接受商用密码检测认证	商用密码检测、认证机构应当依法取得相关资质才能开展检测认证工作	涉及国家安全、国计民生、社会公共利益的商用密码产品必须检测认证合格后，方可销售或者提供

266	多项选择题	根据《商用密码产品认证规则》，以下对商用密码认证证书的说法正确的是（　）。	商用密码产品认证证书的有效期为五年	认证机构定期监督认定不符合证书保持条件的，可以撤销认证证书	认证证书覆盖产品变更的，认证证书有效期不变	认证证书覆盖产品扩展的，认证证书有效期自动终止
267	多项选择题	2023年2月，美国国家标准与技术研究院(NIST)将Ascon算法确立为轻量级加密(LWC)标准，关于该算法和标准的说法，正确的是（　）。	该标准属于国际标准	该标准旨在保护物联网(IoT)创建和传输的信息	通过法律法规规范标准化机构的职责与权限，可以起到推动技术发展和应用的创新进步的重要作用	境内企业研究、进口或使用该算法没有任何程序或条件限制
268	多项选择题	国务院标准化行政主管部门和国家密码管理部门有权制定商用密码国家标准和行业标准。根据《密码法》《标准化法》，制定标准应当在科学技术研究成果和社会实践经验的基础上，深入调查论证，广泛征求意见，需要实现标准的要求有（）。	先进性	科学性	规范性	时效性
269	多项选择题	在对特定密码技术、产品或服务是否符合进出口监管法律时，应关注的法律法规包括（　）。	《密码法》	《对外贸易法》	《出口管制法》	《个人信息保护法》
270	多项选择题	商用密码进口许可清单、出口管制清单是由以下哪些部门联合发布（ ）。	商务部	国家数据局	国家密码管理局	海关总署
271	多项选择题	按照《密码法》《网络安全法》和《关键信息基础设施安全保护条例》等规定，关键信息基础设施运营者需要开展以下（　）工作。	商用密码应用安全性评估	灾难恢复性评估	关键信息基础设施安全检测评估	网络安全等级测评

272	多项选择题	某商用密码检测单位甲在未取得相关资质的情况下擅自开展商用密码检测活动，并从中获利50万。密码管理部门依据《商用密码管理条例》责令其改正，给予警告，并没收违法所得50万，还可并处下列哪些金额的罚款（ ）。	60	100	140	200
273	多项选择题	根据《密码法》，密码管理部门发现关键信息基础设施运营者甲未按照法律规定开展商用密码应用安全性评估，因此责令其改正，并给予警告。但甲认为其安全措施绝对安全，无需进行安全性评估。对此，密码管理部门可对其进行的处罚有（ ）。	直接处50万元罚款	直接处200万元罚款	对直接负责的主管人员处10万罚款	对直接负责的主管人员处20万罚款
274	多项选择题	单位甲欲从事电子政务电子认证服务，但一直未取得相关资质，面对利益诱惑单位甲选择隐瞒相关资质，并最终获利100万元。根据《密码法》，对单位甲的违法行为，下列处罚正确的是（）。	责令甲停止电子政务电子认证服务活动，并给予警告	没收违法所得100万	处200万罚款	处400万罚款
275	多项选择题	甲机构依法取得商用密码检测机构资质，但在开展检测工作中恶意将A公司有关商用密码产品的源代码泄露给B公司，帮助其获取市场竞争优势，依据《密码法》，针对该行为，下列说法正确的是（ ）。	市场监督管理部门可以自行对甲机构实施行政处罚	密码管理部门不可以对甲机构实施行政处罚	可以对甲机构责令改正或者停止违法行为，给予警告，没收违法所得	情节严重的，吊销相关资质
276	多项选择题	A公司为尽快抢占市场，明知其生产的商用密码产品已经被列入网络关键设备和网络安全专用产品目录，在未经过检测认证的情况下就投入市场进行销售，在短短3个月内获利165万元，根据《密码法》，针对该行为，下列正确的表述有（）。	应当责令改正或者停止违法行为	没收违法产品	没收违法所得	可以并处违法所得一倍以上三倍以下罚款
277	多项选择题	根据《密码法》，对未经认定从事电子政务电子认证服务的行为，规定的法律责任有（ ）。	责令改正	责令停止违法行为	警告	没收违法产品和违法所得与罚款

278	多项选择题	某关键信息基础设施运营者未按照要求要求开展商用密码应用安全性评估，导致因商用密码产品存在安全漏洞而产生大规模的用户数据泄露，根据《密码法》，针对该行为，下列正确的表述有（ ）。	对其进行警告	吊销相关资质	对关键信息基础设施的运营者处以罚款	对直接负责的主管人员处以罚款
279	多项选择题	违反《密码法》关于进口许可、出口管制的规定，可进行处罚的主管部门包括：（ ）。	密码管理部门	市场监督管理部门	国务院商务主管部门	海关
280	多项选择题	违反《密码法》相关规定，发生核心密码、普通密码泄露事件的，由保密行政管理部门、密码管理部门建议有关国家机关、单位对（ ）和（ ）依法给予处分或者处理。	单位负责人	直接负责的主管人员	其他直接责任人员	泄露事件的其他参与者
281	多项选择题	甲公司欲从事使用某款具备加密功能数据备份一体机的密码服务，该数据备份一体机目前已经被列入网络关键设备和网络安全专用产品目录，下列哪些表述是正确的（ ）。	由于我国已经取消商用密码产品销售许可，故甲公司可自由提供密码服务	甲公司所使用的该款数据备份一体机应当经过具备资格的机构检测认证合格后才能使用	甲公司提供的密码服务也应当经过商用密码认证机构认证合格	甲公司提供的密码服务需要经过具备资格的机构检测认证，但所涉及的数据备份一体机可以自由使用
282	多项选择题	根据《密码法》，关于我国商用密码标准化体系，下列表述正确的是（ ）。	国家标准由国家密码管理局组织制定	团体标准代号为GM	行业标准需要报国家标准化管理委员会备案	企业标准由商业密码企业制定或企业联合制定
283	多项选择题	根据《密码法》，大众消费类产品所使用的商用密码应当符合的条件包括（ ）。	社会公众可以不受限制地通过常规零售渠道购买	仅供个人使用	不能轻易改变密码功能	只用于加密，不用于认证
284	多项选择题	国家密码管理部门将建立（ ）的密码法律制度体系。	以《密码法》为核心	以《商用密码管理条例》等行政法规为基础	以密码规章和规范性文件为分支	以密码标准为补充

285	多项选择题	某地密码管理部门贾某因与邻居季某素有矛盾，遂在对季某经营的商用密码产品生产企业进行检查的过程中，恶意刁难，严重影响了企业的正常经营，针对贾某的行为，该地密码管理部门应当（　）。	对贾某和季某进行调解	属于民事纠纷，无需密码管理部门介入	对贾某予以行政处分	如果贾某具有中国共产党党员身份，还应当同时予以党纪处分
286	多项选择题	《密码法》明确提出，推进事中事后监管与社会信用体系相衔接，下列举措表述正确的是（　）。	以国家统一社会信用代码为标识，依法依规建立权威、统一、可查询的商用密码市场主体信用记录	推行商用密码从业单位及有关市场主体信用承诺制度，将信用承诺履行情况纳入信用记录	推进信用分级分类监管,依据商用密码从业单位信用情况，在监管方式、抽查比例和频次等方面采取差异化措施	规范认定并设立商用密码市场主体信用“黑名单”,强化失信联合惩戒
287	多项选择题	商用密码事中事后监督的实施主体包括（　）。	市场监管部门	网信部门	商务部门	海关
288	多项选择题	避免商用密码产品检测认证重复检测认证的做法有（　）。	制定并公布网络关键设备和网络安全专用产品目录，避免适用检测认证制度的产品的重复	推动检测认证结果互认，减少某一类产品检测认证项目的重复	对于各类检测认证机构进行合并	将各类检测认证统一并入网络安全审查
289	多项选择题	我国《密码法》规定，对特定商用密码产品实行强制性检测认证，其主要是为了（　）。	维护国家安全的需要	维护社会公共利益的需要	与《网络安全法》规定的网络关键设备和网络安全专用产品强制性检测认证制度衔接一致	保护个人利益

290	多项选择题	《密码法》第24条明确了商用密码从业单位公开标准的技术要求，下列表述正确的是（ ）。	如果执行国家标准、行业标准和团体标准，企业应该公开相应的标准名称和标准编号	如果执行的标准是本企业制定的企业标准，企业除了公开相应的标准名称和标准编号，还应当公开企业产品、服务的技术指标	公开指标的类别和内容由企业根据自身特点自主确定	企业生产的产品和提供的服务应当符合企业自我声明公开标准提出的技术要求
291	多项选择题	当前我国商用密码行业标准的类别包括（ ）。	基础类标准	应用类标准	检测类标准	管理类标准
292	多项选择题	《密码法》在商用密码管理方面的立法思路主要包括（ ）。	贯彻落实行政审批制度改革要求，充分体现非歧视和公平竞争原则	以转变政府职能为核心，管理方式由重事前审批更多地转为事中事后监管	对于关系国家安全和社会公共利益，又难以通过市场机制或者事中事后监管方式进行有效管理的少数事项，规定必要的行政许可和管制措施	进一步削减行政许可数量，最大限度减少对市场活动的直接干预
293	多项选择题	密码管理部门提请有关部门对核心密码、普通密码有关物品和人员提供免检等便利，必须符合的条件包括（ ）。	基于密码工作需要	按照国家有关规定向有关部门提请	提请免检的对象限于核心密码、普通密码有关物品和人员	相关部门推荐
294	多项选择题	在密码工作实践中，可能涉及密码知识产权保护问题的环节有（ ）。	密码技术研究	密码检测认证	密码应用安全性评估	密码安全审查
295	多项选择题	《密码法》和修订的《商用密码管理条例》颁布实施后，商用密码管理体制将更加科学合理，形成的商用密码行政管理体系将涉及的行政级别包括（ ）。	国家	省	市	县

296	多项选择题	对商用密码服务的认识正确的是（　）。	是为他人提供集成、运营、监理等商用密码支持和保障的活动的一类服务	提供商用密码服务应具备相应的商用密码专业技术、技能和设施、人力等资源	典型的商用密码服务包括密码保障系统集成和密码保障系统运营	云服务商可以提供商用密码服务
297	多项选择题	以下属于商用密码产品的有（　）。	商用密码软件	商用密码芯片	商用密码整机	商用密码系统
298	多项选择题	商用密码检测机构开展检测工作应当遵循商用密码管理政策和相关密码标准的要求，遵循（ ）的原则。	保密	独立	客观	公正
299	多项选择题	目前，商用密码使用由行政推进向依法规范应用转变，下列法律法规可以作为依法规范商用密码应用的法律依据的有（ ）。	《密码法》	《网络安全法》	《商用密码管理条例》	《关键信息基础设施安全保护条例》
300	多项选择题	下列属于国家密码管理部门职权范围的有（ ）。	开展商用密码监督管理	行政执法	建立失信企业联合惩戒和守信企业联合激励制度	调查处理商用密码违法违规案件
301	多项选择题	相比于《商用密码管理条例》，《密码法》具有的特点有（ ）。	立法程序更严	效力位阶更高	适用范围更广	更具综合性
302	多项选择题	根据《电子认证服务密码管理办法》，我国对电子认证服务实施许可制。国家密码管理局对电子认证服务系统的要求包括（ ）。	先进性要求	安全性审查	互联互通测试	创新性要求
303	多项选择题	根据《电子认证服务密码管理办法》，申请《电子认证服务使用密码许可证》应当在电子认证服务系统建设完成后,向所在地的省、自治区、直辖市密码管理机构或者国家密码管理局提交的材料包括（　）。	《电子认证服务使用密码许可证申请表》	企业法人营业执照复印件	电子认证服务系统安全性审查相关技术材料	电子认证服务系统互联互通测试相关技术材料
304	多项选择题	《电子认证服务使用密码许可证》载明的内容包括（　）。	许可证编号	电子认证服务提供者名称	许可证有效期限	发证机关和发证日期

305	多项选择题	关于《电子认证服务使用密码许可证》，下列说法正确的是（　）。	有效期为5年	电子认证服务系统通过安全性审查和互联互通测试是颁发《电子认证服务使用密码许可证》的条件	变更电子认证服务提供者，无需更换《电子认证服务使用密码许可证》	使用不符合规定的密钥管理系统提供的密钥来提供服务，可被吊销《电子认证服务使用密码许可证》
306	多项选择题	《商用密码进口许可清单》、《商用密码出口管制清单》制定的法律依据包括（　）。	《密码法》	《出口管制法》	《海关法》	《对外贸易法》
307	多项选择题	根据《商用密码进口许可清单》和《商用密码出口管制清单》，以下关于商用密码进出口的说法正确的是（　）。	商用密码属于两用物项	商用密码都需要申请进出口许可证	商用密码进口受到许可清单管理	商用密码出口受到管制清单管理
308	多项选择题	根据《商用密码进出口许可程序》，下列关于商用密码进出口许可程序，正确的表述包括（　）。	经营者通过省级商务主管部门向商务部提出申请	申请经审查予以许可的，由商务部颁发两用物项和技术进出口许可证	经营者应当向海关出具两用物项和技术进出口许可证办理海关手续	未获许可证的不得开展进出口活动
309	多项选择题	根据《商用密码进口许可清单》，实施进口许可的商用密码应符合以下的情形（　）。	可能涉及国家安全	可能涉及社会公共利益	具有加密保护功能	完全用于安全认证用途
310	多项选择题	按照《商用密码产品认证目录（第一批）》，密码算法应符合的标准有（　）。	《SM4分组密码算法》	《SM3密码杂凑算法》	《SM2密码算法使用规范》	《SM9标识密码算法》
311	多项选择题	按照《商用密码产品认证目录（第一批）》，密码随机数检测应符合的标准有（　）。	《密码随机数生成模块设计指南》	《软件随机数发生器设计指南》	《随机性检测规范》	《密码产品随机数检测要求》
312	多项选择题	按照《关于调整商用密码产品管理方式的公告》和《商用密码产品认证目录（第二批）》，市场监管总局会同国家密码管理局建立国家统一推行的商用密码认证制度，鼓励商用密码产品获得认证。以下属于商用密码产品的有（　）。	可信密码模块	云服务器密码机	随机数发生器	安全浏览器密码模块

313	多项选择题	按照《国家密码管理局关于取消证明事项的通知》和《证明事项取消目录》，以下事项不再要求企业提供或出具书面证明的有（　）。	申请商用密码科研成果审查鉴定的知识产权证明	申请商用密码产品质量检测机构审批时的质量检测能力其它证明	申请商用密码产品出口许可的法人资格证明	申请电子认证使用密码许可证名称变更的名称变更证明
314	多项选择题	根据《关于开展商用密码检测认证工作的实施意见》的规定，商用密码检测认证工作应当坚持的基本原则包括（　）。	统一管理	共同实施	规范有序	保障安全
315	多项选择题	根据《法律、行政法规、国务院决定设定的行政许可事项清单（2023年版）》的规定，下列属于行政许可事项的是（ ）。	商用密码科研成果审查鉴定	商用密码产品质量检测机构审批	电子认证服务使用密码许可	电子政务电子认证服务机构资质认定
316	多项选择题	国家密码管理局于2017年12月公布的《国家密码管理局关于废止和修改部分管理规定的决定》中，废止的管理规定有（　）。	《商用密码产品销售管理规定》	《商用密码产品使用管理规定》	《商用密码科研管理规定》	《境外组织和个人在华使用密码产品管理办法》
317	多项选择题	修订《商用密码管理条例》的总体思路包括（ ）。	坚持创新发展与保障安全相结合	坚持放宽准入与规范监管相结合	处理好条例与相关法律法规的关系	坚持事中与事后监管相结合
318	多项选择题	根据《商用密码管理条例》，以下对商用密码检测机构的表述正确的是（　）。	从事商用密码产品检测活动，向社会出具具有证明作用的数据、结果的机构，应当经国家密码管理部门认定，依法取得商用密码检测机构资质	从事网络与信息系统商用密码应用安全性评估活动，向社会出具具有证明作用的数据、结果的机构，应当经国家密码管理部门认定，依法取得商用密码检测机构资质	申请商用密码检测机构资质，可以向国家密码管理部门提出口头申请	商用密码检测机构应当按照法律、行政法规和商用密码检测技术规范、规则，在批准范围内独立、公正、科学、诚信地开展商用密码检测

319	多项选择题	下列有关《商用密码管理条例》的表述，正确的是（ ）。	国家依法保护商用密码领域的知识产权	行政机关及其工作人员可以利用行政手段强制转让商用密码技术	国家鼓励和支持商用密码科学技术成果转化和产业化应用	国家支持商用密码科学技术自主创新，对作出突出贡献的组织和个人按照国家有关规定予以表彰和奖励
320	多项选择题	根据《商用密码管理条例》，国家鼓励在外商投资过程中基于（ ）开展商用密码技术合作。	自愿原则	商业规则	公平原则	非歧视原则
321	多项选择题	根据《商用密码管理条例》，以下关于商用密码标准化要求，正确的是（ ）。	国家密码管理部门依据职责，建立商用密码标准实施信息反馈和评估机制，对商用密码标准实施进行监督检查	国家推动参与商用密码国际标准化活动，参与制定商用密码国际标准，推进商用密码中国标准与国外标准之间的转化运用	国家鼓励企业、社会团体和教育、科研机构等参与商用密码国际标准化活动	其他领域的标准涉及商用密码的，应当与商用密码国家标准、行业标准保持协调
322	多项选择题	根据《商用密码管理条例》，以下关于商用密码认证机构的表述，正确的是（ ）。	从事商用密码认证活动的机构，应当依法取得商用密码认证机构资质	申请商用密码认证机构资质，应当向地方市场监督管理部门提出书面申请	地方市场监督管理部门在审查商用密码认证机构资质申请时，应当征求国家密码管理部门的意见。	商用密码认证机构应当对其认证的商用密码产品、服务、管理体系实施有效的跟踪调查，以保证通过认证的商用密码产品、服务、管理体系持续符合认证要求

323	多项选择题	根据《商用密码管理条例》，以下有关电子认证的表述，正确的是（ ）。	电子认证服务机构应当按照法律、行政法规和电子认证服务密码使用技术规范、规则，使用密码提供电子认证服务	电子认证服务密码使用技术规范、规则由国家密码管理部门制定并公布	采用商用密码技术从事电子政务电子认证服务的机构，应当经国家密码管理部门认定，依法取得电子政务电子认证服务机构资质	外商投资电子政务电子认证服务，影响或者可能影响国家安全的，应当依法进行网络安全审查。
324	多项选择题	根据《商用密码管理条例》，商用密码的（ ），适用商用密码进出口规定。	过境、转运、通运、再出口	在境外与综合保税区等海关特殊监管区域之间进出	在境外与出口监管仓库之间进出	在境外与保税物流中心之间进出
325	多项选择题	根据《商用密码管理条例》，对（ ）有重大影响的商用密码出口，由国务院商务主管部门会同国家密码管理部门等有关部门报国务院批准。	国家安全	社会公共安全	外交政策	数据安全
326	多项选择题	根据《商用密码管理条例》，密码管理部门和有关部门依法建立推行商用密码经营主体（ ）等机制，以推进商用密码监督管理与社会信用体系的衔接。	信用记录	信用分级分类监管	失信惩戒	信用修复
327	判断题	根据《密码法》，密码工作坚持总体国家安全观，遵循统一领导、分级负责，创新发展、服务大局，依法管理、保障安全的原则。	正确	错误		
328	判断题	根据《密码法》规定，国家机关和涉及密码工作的单位在其职责范围内负责本机关、本单位或者本系统的密码工作。	正确	错误		
329	判断题	按照《密码法》的三级管理架构要求，省、自治区、直辖市的国家密码管理部门负责相应的商用密码管理工作。	正确	错误		

330	判断题	《密码法》中将密码分为核心密码、一般密码和商用密码。	正确	错误		
331	判断题	根据《密码法》，国家对密码实行分类管理。	正确	错误		
332	判断题	根据《密码法》，我国密码管理体制分为两级。	正确	错误		
333	判断题	根据《密码法》，核心密码和普通密码都属于国家秘密。	正确	错误		
334	判断题	根据《密码法》，核心密码、普通密码和商用密码分别对应保护国家秘密中的绝密、机密、秘密三个密级的信息。	正确	错误		
335	判断题	根据《密码法》，核心密码用于保护国家绝密级、机密级、秘密级信息，直接关系国家安全和利益。	正确	错误		
336	判断题	根据《密码法》，商用密码用于保护企业商业秘密和公民个人隐私，不包括政务领域中的工作信息。	正确	错误		
337	判断题	根据《密码法》，商用密码用于保护不属于国家秘密的信息。	正确	错误		
338	判断题	《密码法》规定，市级以上人民政府应当将密码工作纳入本级国民经济和社会发展规划。	正确	错误		
339	判断题	根据《密码法》规定，任何组织或者个人不得利用密码从事危害国家安全、社会公共利益、他人合法权益等违法犯罪活动。	正确	错误		
340	判断题	根据《密码法》，在有线、无线通信中传递的国家秘密信息，应当依照法律、行政法规和国家有关规定使用核心密码、普通密码进行加密保护、安全认证。	正确	错误		

341	判断题	根据《密码法》，密码管理部门依法对密码工作机构的核心密码、普通密码和商用密码工作进行指导、监督和检查。	正确	错误		
342	判断题	根据《密码法》，密码管理部门因工作需要，按照国家有关规定，可以提请公安、交通运输、海关等部门对核心和普通密码有关物品提供免检等便利。	正确	错误		
343	判断题	根据《密码法》规定，密码管理部门和密码工作机构应当定期或者不定期针对其密码工作人员遵守法律和纪律等情况组织开展安全审查。	正确	错误		
344	判断题	根据《密码法》，国家鼓励商用密码技术的研究开发、学术交流、成果转化和推广应用，健全统一、开放、竞争、有序的商用密码市场体系，鼓励和促进商用密码产业发展。	正确	错误		
345	判断题	根据《密码法》规定，商用密码的科研、生产、销售、服务和进出口，不得损害国家安全、社会公共利益或者他人合法权益。	正确	错误		
346	判断题	根据《密码法》，商用密码进出口单位不属于商用密码从业单位。	正确	错误		
347	判断题	根据《密码法》，商用密码生产单位属于商用密码从业单位。	正确	错误		
348	判断题	根据《密码法》，商用密码国家标准的相关技术要求一般应高于行业标准、团体标准和企业标准。	正确	错误		
349	判断题	根据《密码法》，国家推动参与商用密码国际标准化活动，参与制定商用密码国际标准，推进商用密码中国标准与国外标准之间的转化运用。	正确	错误		

350	判断题	根据《密码法》规定，商用密码从业单位开展商用密码活动，应当符合有关法律、行政法规、商用密码强制性国家标准以及该从业单位公开标准的技术要求。	正确	错误		
351	判断题	根据《密码法》，商用密码产品检测认证适用《中华人民共和国数据安全法》的有关规定，避免重复检测认证。	正确	错误		
352	判断题	根据《密码法》规定，商用密码服务使用网络关键设备和网络安全专用产品的，应当经商用密码认证机构对该商用密码服务认证合格。	正确	错误		
353	判断题	根据《密码法》规定，所有商用密码产品都必须由具备资格的机构检测认证合格后，方可销售或者提供。	正确	错误		
354	判断题	根据《密码法》规定，商用密码应用安全性评估应当与关键信息基础设施安全检测评估、网络安全等级测评制度相衔接，避免重复评估、测评。	正确	错误		
355	判断题	根据《密码法》规定，关键信息基础设施运营者必须请商用密码检测机构开展密评。	正确	错误		
356	判断题	根据《密码法》规定，关键信息基础设施的运营者采购涉及商用密码的网络产品和服务，可能影响国家安全的，应当按照《中华人民共和国行政许可法》的规定，通过国家网信部门会同国家密码管理部门等有关部门组织的国家安全审查。	正确	错误		
357	判断题	根据《密码法》规定，法律、行政法规和国家有关规定要求使用商用密码进行保护的关键信息基础设施，其运营者应当使用普通密码进行保护。	正确	错误		

358	判断题	根据《密码法》规定，大众消费类产品所采用的商用密码也要实行进口许可和出口管制制度。	正确	错误		
359	判断题	根据《密码法》规定，车载蓝牙中的密码模块属于大众消费类产品所采用的商用密码。	正确	错误		
360	判断题	根据《密码法》规定，国家密码管理部门对采用商用密码技术从事电子政务电子认证服务的机构进行认定，会同有关部门负责政务活动中使用电子签名、数据电文的管理。	正确	错误		
361	判断题	根据《密码法》，各省的商用密码行业协会是社会团体组织。	正确	错误		
362	判断题	根据《密码法》，商用密码领域的行业协会等组织依照法律、行政法规及其章程的规定，为商用密码从业单位提供信息、技术、培训等服务。	正确	错误		
363	判断题	根据《密码法》规定，密码管理部门和有关部门及其工作人员应对其在履行职责中知悉的商业秘密和个人隐私严格保密。	正确	错误		
364	判断题	根据《密码法》规定，密码管理部门和有关部门及其工作人员不得要求商用密码从业单位和商用密码检测、认证机构向其披露源代码等密码相关专有信息。	正确	错误		
365	判断题	根据《密码法》规定，窃取他人加密保护的信息，非法侵入他人的密码保障系统，由有关部门依照《中华人民共和国网络安全法》和其他有关法律、行政法规的规定追究法律责任。	正确	错误		

366	判断题	某人非法侵入了国防军工企业的密码保障系统，有关部门将依照《中华人民共和国网络安全法》和其他有关法律、行政法规的规定追究其法律责任。	正确	错误		
367	判断题	根据《密码法》规定，发生核心密码、普通密码泄密案件的，由保密行政管理部门、密码管理部门直接对负责的主管人员和其他直接责任人员依法给予处分或者处理。	正确	错误		
368	判断题	根据《密码法》规定，某单位提供了检测认证不合格的商用密码产品，将由市场监督管理部门会同密码管理部门进行处罚。	正确	错误		
369	判断题	根据《密码法》规定，某关键信息基础设施的运营者未按照要求开展商用密码应用安全性评估，导致危害网络安全后果的，该运营者将面临五万元以上五十万元以下罚款。	正确	错误		
370	判断题	根据《密码法》，关键信息基础设施的运营者使用未经安全审查的产品或者服务的，由国务院商务主管部门责令停止使用，处采购金额一倍以上十倍以下罚款。	正确	错误		
371	判断题	违反《密码法》规定实施商用密码进口许可、出口管制的，可以由海关或者国务院商务主管部门或国家密码管理部门依法予以处罚。	正确	错误		
372	判断题	根据《密码法》，某密码管理部门的工作人员在密码工作中非法向他人提供在履行职责中知悉的商业秘密和个人隐私的，该人员将被依法给予处分。	正确	错误		
373	判断题	违反《密码法》规定，构成犯罪的，依法追究刑事责任；给他人造成损害的，依法承担民事责任。	正确	错误		

374	判断题	根据《密码法》规定，利用密码从事危害国家安全、社会公共利益、他人合法权益等活动，情节严重，构成犯罪的，依法追究刑事责任。	正确	错误		
375	判断题	我国《密码法》的正式颁布日期是2019年10月26日，自颁布之日起施行。	正确	错误		
376	判断题	按照《密码法》的要求，坚持党对密码工作的绝对领导是在任何时候、任何情况下都必须毫不动摇坚持的根本原则。	正确	错误		
377	判断题	根据《密码法》，国家对商用密码产品的科研、生产、销售和使用实行专控管理。	正确	错误		
378	判断题	根据《密码法》，我国商用密码检测认证方式以强制检测认证为原则，自愿检测认证为例外。	正确	错误		
379	判断题	《密码法》中的商用密码产品市场准入管理制度充分体现了行政审批制度改革精神，与《网络安全法》第二十三条的规定是衔接一致的。	正确	错误		
380	判断题	根据《密码法》，大众消费类产品所采用的商用密码，是可以不受限制地通过常规零售渠道购买并能轻易改变密码功能的产品或技术。	正确	错误		
381	判断题	根据《密码法》，电子政务电子认证服务机构认定制度与《电子签名法》中的电子认证服务许可存在重复许可的可能。	正确	错误		
382	判断题	根据《密码法》，商用密码日常监管中的“双随机、一公开”中的“双随机”，意思是随机抽取密码管理部门和选派执法检查人员。	正确	错误		
383	判断题	1999年，国务院正式公布《商用密码管理条例》，自公布之日起施行。商用密码的名称开始为社会所熟知和广泛使用。	正确	错误		

384	判断题	根据《商用密码应用安全性评估管理办法（试行）》，关键信息基础设施运营者在系统开始运行前，不必组织开展商用密码应用安全性评估工作。	正确	错误		
385	判断题	根据《商用密码应用安全性评估管理办法（试行）》，商用密码应用安全性评估工作由国家密码管理部门认定的密码测评机构承担，国家密码管理部门定期发布测评机构目录。	正确	错误		
386	判断题	根据《商用密码应用安全性评估管理办法（试行）》，对于关键信息基础设施，测评机构可将商用密码应用安全性评估与关键信息基础设施网络安全测评、网络安全等级保护测评同步进行。	正确	错误		
387	判断题	根据《商用密码应用安全性评估管理办法（试行）》，网络安全等级保护第三级及以上信息系统完成规划、建设、运行和应急评估后，应在30个工作日内将评估结果报主管部门及所在地区(部门)密码管理部门备案，并将评估结果同时报所在地区公安部门备案。	正确	错误		
388	判断题	根据《商用密码应用安全性评估管理办法（试行）》，测评机构完成商用密码应用安全性评估工作后，应在30个工作日内将评估结果报国家密码管理部门备案，并将评估结果同时报国务院公安部门备案。	正确	错误		
389	判断题	根据《商用密码应用安全性评估管理办法（试行）》，涉及国家安全和社会公共利益的重要领域网络和信息系统的建设单位应对评估工作承担管理责任，并接受密码管理部门的监督、检查和指导。	正确	错误		

390	判断题	根据《商用密码应用安全性评估管理办法（试行）》，国家密码管理部门根据工作需要，不定期对各地区(部门)商用密码应用安全性评估工作开展检查，并对有关重要领域网络和信息系统进行抽查。	正确	错误		
391	判断题	根据《商用密码应用安全性测评机构管理办法（试行）》，申请成为商用密码应用安全性测评机构的单位应具备完善的人员结构，且通过“商用密码应用安全性测评人员考核”的测评人员数量不少于5人。	正确	错误		
392	判断题	根据《商用密码应用安全性测评机构管理办法（试行）》，申请成为商用密码应用安全性测评机构的单位注册资金应在500万元以上。	正确	错误		
393	判断题	根据《商用密码应用安全性测评机构管理办法（试行）》，申请成为商用密码应用安全性测评机构的单位，测评工作场地应不少于200平方米。	正确	错误		
394	判断题	根据《商用密码应用安全性测评机构管理办法（试行）》，已经申请成为商用密码应用安全性测评机构的单位及直接控股的母公司或子公司可以从事商用密码产品检测认证工作。	正确	错误		
395	判断题	根据《商用密码应用安全性测评机构管理办法（试行）》，成立年限在一年以上，从事信息系统安全相关工作半年以上的单位可以申请成为商用密码应用安全性测评机构。	正确	错误		
396	判断题	根据《商用密码应用安全性测评机构管理办法（试行）》，通过商用密码应用安全性测评机构初审的申请单位,应在60个工作日内参加培训、考核和能力评审。	正确	错误		

397	判断题	根据《商用密码应用安全性测评机构管理办法（试行）》，申请商用密码应用安全性测评机构的单位应当确保本单位测评人员全程参加测评人员培训、考核工作。	正确	错误		
398	判断题	根据《商用密码应用安全性测评机构管理办法（试行）》，商用密码应用安全性测评机构名称地址、主要负责人发生变更时，测评机构应在15个工作日内向国家密码管理局报告。	正确	错误		
399	判断题	根据《商用密码应用安全性测评机构管理办法（试行）》，国家密码管理局、测评机构所属省部密码管理局对测评机构负有监督检查职责，应定期开展强制测评机构检查工作。	正确	错误		
400	判断题	根据《商用密码应用安全性测评机构管理办法（试行）》，如果商用密码应用安全性测评机构的测评人员未通过培训考核，就开始从事商用密码应用安全性评估工作，国家密码管理局将责令其限期整改。	正确	错误		
401	判断题	根据《商用密码应用安全性测评机构管理办法（试行）》，如果商用密码应用安全性测评机构因单位股权、人员等情况发生变动，不符合商用密码应用安全性测评机构基本条件的，国家密码管理局将责令其限期整改。	正确	错误		
402	判断题	根据《商用密码应用安全性测评机构管理办法（试行）》，某商用密码应用安全性测评机构故意泄露被测评单位工作秘密、重要信息系统数据信息，国家密码管理局应取消其商用密码应用安全性测评机构试点资格。	正确	错误		

403	判断题	根据《商用密码应用安全性测评机构管理办法（试行）》，某商用密码应用安全性测评机构的测评人员未经允许擅自使用商用密码应用安全性评估工作中收集的数据信息，且情形特别严重，应将其从商用密码应用安全性测评人员名单中移除，并对其所在测评机构进行通报。	正确	错误		
404	判断题	根据《电子认证服务密码管理办法》，电子认证服务系统所需密钥服务由国家密码管理局和省、自治区、直辖市密码管理机构规划的密钥管理系统提供。	正确	错误		
405	判断题	根据《电子认证服务密码管理办法》，申请《电子认证服务使用密码许可证》时，应向所在地的省、自治区、直辖市密码管理机构或者国家密码管理局提交的材料中不包括电子认证服务系统互联互通测试相关技术材料。	正确	错误		
406	判断题	《电子认证服务使用密码许可证》有效期为5年。	正确	错误		
407	判断题	电子认证服务提供者终止电子认证服务的,原持有的《电子认证服务使用密码许可证》将在15个工作日内失效。	正确	错误		
408	判断题	按照《商用密码进口许可清单》要求，进口清单所列物项和技术中，加密通信速率1Gbps的VPN设备不属于应向商务部申请办理两用物项和技术进口许可证的密码产品。	正确	错误		
409	判断题	根据《密码法》的有关规定，商务部、国家密码管理局、海关总署制定了《商用密码出口管制清单》。	正确	错误		

410	判断题	《密码法》正式颁布时间为2019年10月26日。	正确	错误		
411	判断题	外国投资者可以基于自愿原则和商业规则在中国开展商用密码技术合作。	正确	错误		
412	判断题	商用密码技术审查鉴定的范围包括密码算法、密码协议、密钥管理机制等商用密码技术的内容。	正确	错误		
413	判断题	如果某企业承诺适用自我声明公开的企业标准的技术要求，则其应该符合该标准。	正确	错误		
414	判断题	商用密码应用安全性评估属于商用密码认证活动。	正确	错误		
415	判断题	申请商用密码检测机构资质应向国家密码管理部门提出。	正确	错误		
416	判断题	申请商用密码认证机构资质应向国务院市场监督管理部门提出。	正确	错误		
417	判断题	使用商用密码检测机构出具的检测数据的单位，应对检测数据的真实性、准确性负责。	正确	错误		
418	判断题	国务院市场监督管理部门在审查商用密码认证机构资质申请时，可直接依据《认证认可条例》做出决定，无需征求国家密码管理部门的意见。	正确	错误		
419	判断题	商用密码检测机构、商用密码认证机构都应当具备与从事活动相适应的技术能力。	正确	错误		
420	判断题	未经取得国家密码管理部门同意使用密码的证明文件，任何单位不得采用商用密码技术提供电子认证服务。	正确	错误		

421	判断题	采用商用密码技术从事电子政务电子认证服务的机构，应当经国务院市场监督管理部门认定，依法取得电子政务电子认证服务机构资质。	正确	错误		
422	判断题	取得电子政务电子认证服务机构资质，应当具有为政务活动提供年度电子政务电子认证服务的能力。	正确	错误		
423	判断题	负责国家电子认证信任源的规划和管理的是国家密码管理部门和国务院工业和信息化部门。	正确	错误		
424	判断题	是否涉及国家安全、社会公共利益是判定商用密码进口许可、出口管制的重要依据。	正确	错误		
425	判断题	国家支持商用密码在人工智能的模型、算法和数据保护中的规范应用。	正确	错误		
426	单项选择题	根据《密码法》和《网络安全法》，某黑客为炫耀技术能力，非法侵入他人的密码保障系统，则有权对其进行行政处罚的部门是（ ）。	密码管理部门	公安机关	网信部门	工信部门
427	单项选择题	根据《密码法》和《网络安全法》，某黑客为炫耀技术能力，非法侵入他人的密码保障系统并受到治安管理处罚，则公安机关能够对其进行的行政处罚包括（ ）。	使其终身不得从事网络运营关键岗位	使其二十年内不得从事网络运营关键岗位	使其十年内不得从事网络运营关键岗位	使其五年内不得从事网络运营关键岗位
428	单项选择题	根据《标准化法》，关于商用密码标准体系，下列说法错误的是（ ）。	商用密码国家标准可能有强制性标准和推荐性标准	商用密码行业标准可能有强制性标准和推荐性标准	商用密码团体标准由社会团体制定，只能是推荐性标准	商用密码企业标准由商用密码企业制定或企业联合制定
429	单项选择题	《国家政务信息化项目建设管理办法》适用的国家政务信息系统包括（ ）。	国家重点业务信息系统	国家信息资源库	国家信息安全基础设施	以上都是
430	单项选择题	根据《国家政务信息化项目建设管理办法》，（ ）负责牵头编制国家政务信息化建设规划，对各部门审批的国家政务信息化项目进行备案管理。	国家发展改革委	财政部	国务院办公厅	中央网信办

431	单项选择题	根据《国家政务信息化项目建设管理办法》，可以直接编报项目可行性研究报告的项目是（ ）。	党中央、国务院有明确要求的项目	已经纳入国家政务信息化建设规划的项目	涉及国家重大战略、国家安全等特殊原因的项目	前期工作深度达到规定要求的项目
432	单项选择题	根据《国家政务信息化项目建设管理办法》，对于已经纳入国家政务信息化建设规划的项目，以下环节可以简化掉的是（ ）。	编报项目建议书	编报可行性研究报告	编报初步设计方案	编报框架方案
433	单项选择题	根据《国家政务信息化项目建设管理办法》，有关部门自行审批新建、改建、扩建的国家政务信息化项目，应当按规定履行审批程序并向国家发展改革委备案。其中改建、扩建项目还需提交前期项目（ ）。	第三方后评价报告	密码应用安全性评估报告	第三方审计报告	安全风险评估报告
434	单项选择题	按照《国家政务信息化项目建设管理办法》，以下有关国家政务信息化项目建设单位的规划和审批管理要求，错误的是（ ）。	编制信息资源目录	建立信息共享长效机制	共享信息使用情况反馈机制	将数据仅向特定企业、社会组织开放
435	单项选择题	根据《国家政务信息化项目建设管理办法》，以下关于国家政务信息化项目建设过程中的信息资源共享的表述，错误的是（ ）。	可行性研究报告、初步设计方案应当包括信息资源共享分析篇（章）	咨询评估单位的评估报告应当包括对信息资源共享分析篇（章）的评估意见	审批部门的批复文件或者上报国务院的请示文件应当包括对信息资源共享分析篇（章）的意见	项目建设单位可以将应当普遍共享的数据仅向特定企业、社会组织开放
436	单项选择题	根据《国家政务信息化项目建设管理办法》，国家政务信息化项目建设单位应当落实国家密码管理有关法律法规和标准规范的要求，同步规划、同步建设、同步运行（ ）。	网络安全保障系统	密码保障系统	技术保障系统	以上都是
437	单项选择题	按照《国家政务信息化项目建设管理办法》，下列不属于国家政务信息化项目验收的重要内容的是（ ）。	项目软硬件产品的安全可靠情况	项目密码应用和安全审查情况	硬件设备和新建数据中心能源利用效率情况	项目定期安全评估情况

438	单项选择题	根据《国家政务信息化项目建设管理办法》，国家政务信息化项目建设单位在建设期内每年年底前向项目审批部门提交的项目绩效评价报告包括（ ）。	建设进度	投资计划执行情况	已投入试运行系统的试运行效果及遇到的问题	以上都是
439	单项选择题	根据《国家政务信息化项目建设管理办法》，对于因开展需求分析、编制可行性研究报告和初步设计、购地、拆迁等确需提前安排投资的政务信息化项目，项目建设单位可以在项目可行性研究报告获批复（ ），向项目审批部门提出申请。	前	后	同时	7个工作日内
440	单项选择题	根据《国家政务信息化项目建设管理办法》，国家政务信息化项目建成后（ ）内，项目建设单位应当按照国家有关规定申请审批部门组织验收。	一年	三个月	半年	九个月
441	单项选择题	根据《国家政务信息化项目建设管理办法》，项目建设单位应当在项目通过验收并投入运行后（ ）内，依据国家政务信息化建设管理绩效评价有关要求，开展自评价，并将自评价报告报送项目审批部门和财政部门。	12至24个月	6至12个月	一年	半年
442	单项选择题	根据《国家政务信息化项目建设管理办法》，有关项目建设单位新建、改建、扩建政务信息系统的表述，错误的是（ ）。	对于未按要求共享数据资源或者重复采集数据的政务信息系统，项目建设单位不得新建、改建、扩建政务信息系统	对于未纳入国家政务信息系统总目录的系统，项目建设单位不得新建、改建、扩建政务信息系统	对于不符合密码应用和网络安全要求的系统，项目建设单位不得新建、改建、扩建政务信息系统	对于存在重大安全隐患的政务信息系统，项目建设单位不得新建、改建、扩建政务信息系统
443	单项选择题	根据《国家政务信息化项目建设管理办法》网络安全监管部门应当依法加强对国家政务信息系统的安全监管，并指导监督项目建设单位落实（ ）。	网络安全审查制度要求	网络安全监管要求	四同步要求	网络安全监测预警与信息通报要求

444	单项选择题	《网络安全法》规定，网络运营者应当按照网络安全等级保护制度的要求，履行网络安全保护义务，对（　）采取加密措施。	所有数据	一般数据	重要数据	网络日志
445	单项选择题	按照《网络安全法》的要求，关键信息基础设施的运营者应当（　）对其网络的安全性和可能存在的风险开展检测评估。	自行	自行或者委托网络安全服务机构	委托网络安全服务机构	自行并且委托网络安全服务机构
446	单项选择题	按照《网络安全法》的要求，关键信息基础设施的运营者应当对其网络的安全性和可能存在的风险（　）检测评估。	每三个月至少一次	每半年至少进行一次	每年至少进行一次	每两年至少一次
447	单项选择题	某市所属企业为国家政务系统提供运维服务，对其服务过程中产生的大量政务数据不采取加密措施，根据《数据安全法》，可对其实施的处置及处罚措施不包括（　）。	当地公安机关责令其限期整改	当地公安机关对其给予警告的处罚	若该单位拒不改正则当地公安机关可对其进行五百万元罚款	当地公安机关对其处以三十万元罚款
448	单项选择题	某国家机关以明文形式传输大量重要数据，致使数据被黑客窃取后通过暗网在境外销售，按照《数据安全法》的内容，对此下列说法正确的是（）。	有关主管部门有权对其进行警告	有关主管部门有权责令其整改	有关主管部门有权对其处以罚款	有关主管部门对直接负责的主管人员依法给予处分
449	单项选择题	根据《个人信息保护法》规定，要求个人信息处理者使用密码保护（　）。	等保第三级以上网络	关键信息基础设施	个人信息	重要数据
450	单项选择题	某科技信息公司存有大量个人信息，根据《个人信息保护法》要求，该公司应采取的保护措施，下列说法正确的是（　）。	制定内部管理制度	定期对从业人员进行安全教育和培训	采取相应的加密、去标识化等措施	以上都是
451	单项选择题	按照《个人信息保护法》，某市网约车企业以明文形式存有大量敏感个人信息，后个人信息被境外黑客获取进行售卖，情节严重，则对其进行的处罚，下列说法正确的是（　）。	因其认错态度较好且及时改正，公安机关仅对其进行警告	当地网信部门对其直接责任人员处以二百万元罚款	所属省级公安机关对其进行一千万元的罚款	当地网信部门对其进行三千万元的罚款

452	单项选择题	按照《数据安全法》和《商用密码应用与安全性评估》的内容，关于使用密码技术保护数据和系统的做法正确的是（　）。	某科技有限公司在重要数据传输过程中使用商用密码技术进行加密传输	某科技公司在数据存储阶段使用MD5算法对重要数据进行加密	某关键信息基础设施运营者使用核心密码保护重要数据	某银行的重要数据使用核心密码进行加密保护
453	单项选择题	根据《关键信息基础设施安全保护条例》，（）对关键信息基础设施中的密码使用和管理进行监管。	国家互联网信息办公室	海关总署	国家密码管理局	国家数据局
454	单项选择题	《信息安全等级保护管理办法》规定，信息系统的安全保护等级分为（　）级。	三	四	五	六
455	单项选择题	《信息安全等级保护管理办法》规定，信息系统受到破坏后，会对（　）造成特别严重损害的，属于第五级。	公民、法人和其他组织的合法权益	社会秩序	公共利益	国家安全
456	单项选择题	《信息安全等级保护管理办法》规定，（　）对第四级信息系统信息安全等级保护工作进行强制监督、检查。	国家网信部门	国家信息安全监管部门	国家密码管理部门	工业和信息化部
457	单项选择题	《信息安全等级保护管理办法》规定，国家指定专门部门对第（　）级信息系统信息安全等级保护工作进行专门监督、检查。	三	四	五	六
458	单项选择题	《信息安全等级保护管理办法》规定，对拟确定为第（　）级以上信息系统的，运营、使用单位或者主管部门应当请国家信息安全保护等级专家评审委员会评审。	二	三	四	五
459	单项选择题	《信息安全等级保护管理办法》规定，第三级信息系统应当（　）至少进行一次等级测评。	每半年	每年	每一年半	每两年
460	单项选择题	《信息安全等级保护管理办法》规定，第四级信息系统应当（　）至少进行一次等级测评。	每三个月	每半年	每年	每一年半
461	单项选择题	《信息安全等级保护管理办法》规定，第五级信息系统应当（　）进行等级测评。	每三个月	每半年	每年	依据特殊安全需求

462	单项选择题	《信息安全等级保护管理办法》规定，第三级信息系统应当（ ）至少进行一次自查。	每半年	每年	每一年半	每两年
463	单项选择题	《信息安全等级保护管理办法》规定，第四级信息系统应当（ ）至少进行一次自查。	每三个月	每半年	每年	每一年半
464	单项选择题	《信息安全等级保护管理办法》规定，新建第二级以上信息系统，应当在投入运行后（ ）办理备案手续。	10日内	20日内	30日内	60日内
465	单项选择题	《信息安全等级保护管理办法》规定，信息系统备案后，对符合等级保护要求的，公安机关应当在收到备案材料之日起的（ ）内颁发信息系统安全等级保护备案证明。	10个工作日内	20个工作日内	30个工作日内	60个工作日内
466	单项选择题	《信息安全等级保护管理办法》规定，国家密码管理部门负责等级保护工作中有关（ ）的监督、检查、指导。	等保工作	密码工作	保密工作	部门间协调工作
467	单项选择题	根据《信息安全等级保护管理办法》规定，在等级保护工作中，采用密码对不涉及国家秘密的信息和信息系统进行保护的，其密码的配备使用情况应当（ ）。	向国家密码管理机构备案	经国家密码管理机构审批	经国务院公安部门审批	向国务院公安部门备案
468	单项选择题	《信息安全等级保护管理办法》规定，企业使用密码技术对信息系统进行系统等级保护建设和整改过程中，下列行为错误的是（ ）。	采用经国家密码管理部门批准使用的密码产品进行安全保护	采用经国家密码管理部门准于销售的密码产品进行安全保护	采用国外引进的密码产品	经批准采用含有加密功能的进口信息技术产品
469	单项选择题	《信息安全等级保护管理办法》规定，为节省成本，小企业不涉密信息系统中的密码应用的测评工作可以由（ ）进行测评。	我国专业过硬的网络安全技术专家	国家密码管理局发布的密评试点机构	国家认可的不具有密评资质的等保测评机构	某个有专门技术团队的政府部门
470	单项选择题	《信息安全等级保护管理办法》规定，（ ）可以定期或者不定期对信息系统等级保护工作中密码配备、使用和管理的情况进行检查和测评。	省级密码管理部门	市级密码管理部门	县级密码管理部门	以上都对

471	单项选择题	根据《信息安全等级保护管理办法》规定，某企业有重要涉密信息系统，其密码配备、使用和管理情况，有关部门应（ ）至少进行一次检查和测评。	每两年	每年	每六个月	每三个月
472	单项选择题	根据《中国禁止出口限制出口技术目录》，（ ）不属于我国限制出口的量子密码技术。	量子密码实现方法	量子密码工程实现技术	量子密码的传输技术	量子密码的对抗技术
473	单项选择题	根据《中国禁止出口限制出口技术目录》，（ ）不属于我国限制出口的密码芯片设计和实现技术。	高速密码算法	祖冲之序列密码算法	并行加密技术	密码芯片的安全设计技术
474	单项选择题	根据《电子签名法》规定，从事电子认证服务，应当向（ ）提出申请。	国务院信息产业主管部门	国务院公安部门	国家密码管理部门	国家市场监管总局
475	单项选择题	根据《电子签名法》规定，有关主管部门接到从事电子认证服务申请后经依法审查，征求（ ）等有关部门意见后，在一定期限内作出许可或者不予许可的决定。	国务院商务主管部门	国家数据局	国家科技委员会	国家网信部门
476	多项选择题	按照《网络安全审查办法》的内容，某国家机关系被认定的关键信息基础设施运营者，其欲采购某款境外设计的商用密码产品，下列表述正确的是（ ）。	该国家机关应当首先自行预判该商用密码产品是否可能产生国家安全风险	如果该国家机关认为使用该商用密码产品可能产生国家安全风险，应当申报网络安全审查	如果国家密码管理局认为使用该商用密码产品可能产生国家安全风险，网络安全审查办公室可以依职权对该国家机关启动网络安全审查	由于该国家机关采购的是境外设计的商用密码产品，故只能通过国家机关申请来启动网络安全审查，网络安全审查办公室无权自行启动网络安全审查
477	多项选择题	根据《网络安全审查办法》，申报商用密码国家安全审查，关键基础设施运营者应当提供的申报材料包括（ ）。	申报书	采购文件或协议	关于影响或者可能影响国家安全的分析报告	网络安全审查工作需要的其他材料

478	多项选择题	国家密码管理局在日常检查中发现，某市一军工科研单位的系统已被列入关键信息基础设施，其在2022年采购了一批境外A公司生产的商用密码产品，但并未申报网络安全审查。国家密码管理局发现A公司具有从事网络间谍的前科，则下列表述正确的是（　）。	国家密码管理局应当立即启动网络安全审查	国家密码管理局应当告知该军工科研单位自行申报网络安全审查	应当由网络安全审查办公室启动网络安全审查，国家密码管理局无权自行启动网络安全审查	网络安全审查办公室应当报请中央网络安全和信息化委员会批准，才能够启动网络安全审查
479	多项选择题	按照《网络安全审查办法》，网络安全审查办公室拟对某关键基础设施运营者采购商用密码产品开展网络安全审查工作，其应当重点评估的因素有（　）。	该商用密码产品使用后带来的关键信息基础设施被非法控制、遭受干扰或者破坏的风险	该商用密码产品供应中断对关键信息基础设施业务连续性的危害	该商用密码产品的安全性、开放性、透明性、来源的多样性	该商用密码产品提供者遵守我国法律、行政法规、部门规章情况
480	多项选择题	根据《网络安全审查办法》，针对某关键信息基础设施采购商用密码产品的活动，网络安全审查工作机制成员单位、相关部门无法形成是否存在国家安全风险的一致性意见，下列相关表述是正确的是（　）。	网络安全审查办公室应当作出允许采购的决定	网络安全审查办公室应当启动特别审查程序处理	网络安全审查办公室应当再次形成审查结论建议	再次形成的审查结论建议应当报请中央网络安全和信息化委员会批准
481	多项选择题	对于在安全研究中发现的密码安全漏洞，在确定是否与境外安全社区共享时，应符合的法律法规和规定包括（　　）。	《密码法》	《出口管制法》	《网络产品安全漏洞管理规定》	《数据安全法》
482	多项选择题	根据《电子签名法》，当事人约定使用电子签名、数据电文的文书，不得仅因为其采用电子签名、数据电文的形式而否定其法律效力。但下列文书除外的有（　）。	涉及婚姻、收养、继承等人身关系的	涉及停止供水、供热、供气等公用事业服务的	涉及财产交易的民事合同	涉及房屋确权的单证文书

483	多项选择题	按照《电子签名法》的内容，关于数据电文的发送、接收时间，下列说法正确的是（　　）。	数据电文进入发件人控制之外的某个信息系统的时间，视为该数据电文的发送时间	收件人指定特定系统接收数据电文的，数据电文进入该特定系统的时间视为该数据电文的接收时间	未指定特定系统的，数据电文进入收件人的任何系统的首次时间，视为该数据电文的接收时间	当事人对数据电文的发送时间、接收时间另有约定的，从其约定
484	多项选择题	根据《电子签名法》规定，数据电文需要被视为满足法律、法规规定的原件形式应符合的要求包括（　）。	能够有效地表现所载内容	能够可靠地保证自最终形成时起，内容保持完整、未被更改	在数据电文上增加背书以及数据交换、储存和显示过程中发生的形式变化不影响数据电文的完整性	可供随时调取查用
485	多项选择题	根据《电子签名法》规定，电子签名可以被视为可靠的电子签名，应当满足的条件包括（　）。	电子签名制作数据用于电子签名时，属于电子签名人专有	签署时电子签名制作数据仅由电子签名人控制	签署后对电子签名的任何改动能够被发现	签署后对数据电文内容和形式的任何改动能够被发现
486	多项选择题	按照《电子签名法》，下列关于电子签名的表述正确的是（　　）。	可靠的电子签名其法律效力仅次于手写签名或者盖章	电子签名人知悉电子签名制作数据可能已经失密时，应当终止使用该电子签名制作数据	只要符合双方约定，当事人也可自行选择使用电子签名	境外电子认证服务提供者在境外签发的电子签名认证证书与依据本法认证的电子签名认证证书具有同等法律效力
487	多项选择题	根据《电子签名法》的规定，提供电子认证服务的主体应当具备的条件包括（　）。	具有与提供电子认证服务相适应的专业技术人员和管理人员	具有与提供电子认证服务相适应的资金和经营场所	具有符合国家安全标准的技术和设备	具有国家密码管理机构同意使用密码的证明文件

488	多项选择题	根据《电子签名法》规定，电子认证服务提供者签发的电子签名认证证书应当准确无误，并应当载明的内容包括（　）。	电子认证服务提供者名称	证书持有人名称	证书持有人的电子签名验证数据	电子认证服务提供者的电子签名
489	多项选择题	根据《电子签名法》规定，开展电子认证服务应当遵循的规范要求包括（　）。	依法制定并公布电子认证业务规则	签发证书应查验申请人身份并对有关材料进行审查，确保所签发的证书准确无误，确保证书内容在有效期内完整、准确	暂停或者终止服务前应就业务承接及其他有关事项进行妥善安排	妥善保存与认证相关的信息
490	多项选择题	根据《网络安全法》，国家实行网络安全等级保护制度，网络运营者应当按照要求履行安全保护义务，除实施加密措施外，安全保护义务还包括（　）。	确定网络安全负责人	采取防范网络攻击的技术措施	数据分类	重要数据备份
491	多项选择题	A平台系大型网络电商平台，为更好地形成“用户画像”，要求对于用户交易数据不实行加密，后因受到第三方网络攻击而导致用户数据大规模泄露。针对这一情况，下列表述正确的是（　）。	我国立法中没有明确规定，故不属于违法行为	违反《网络安全法》关于网络安全保护的规定	由于用户数据泄露系第三方网络攻击造成，故A平台不承担法律责任	对A平台及其直接负责的主管人员均应当处以罚款
492	多项选择题	2017年，Wannacry病毒席卷全球，该款勒索软件通过加密受害者信息系统中的重要文件，强迫受害者支付赎金。我国能够用于规制该勒索行为的现行立法包括（　）。	《密码法》	《网络安全法》	《刑法》	《治安管理处罚法》
493	多项选择题	商用密码产品和服务提供者应当承担必要的产品和服务安全义务，下列行为会导致商用密码产品和服务提供者承担相应的法律责任的有（　）。	设置恶意程序	对其产品、服务存在的安全缺陷、漏洞等风险未立即采取补救措施	未按照规定及时告知用户并向有关主管部门报告	擅自终止为其产品、服务提供安全维护

494	多项选择题	某漏洞平台擅自将挖掘的某款商用密码产品漏洞公布在自己的网站上，导致短时期内该款商用密码产品遭受到大量利用披露漏洞的攻击活动，针对这一行为，下列表述正确的是（ ）。	该平台披露漏洞的行为无主观恶意，故不需要承担法律责任	不得在商用密码产品提供者提供漏洞修补措施之前发布漏洞信息	主管部门可责令该平台暂停相关业务	可对该平台的直接负责主管人员和其他直接责任人员处以罚款
495	多项选择题	甲系一名商用密码产品的设计人员，受Wannacry事件启发，甲认为加密勒索是一项“来钱快”的生财之道，但自己又没有直接实施勒索的勇气，遂在网上兜售自己开发的加密勒索软件工具。针对这一事实，下列表述正确的是（ ）。	甲没有直接实施勒索活动，故不构成网络违法犯罪行为	甲如果违法情节轻微，仅受到治安管理处罚，则五年内不得从事网络安全管理和网络运营关键岗位的工作	甲如果违法情节严重，受到刑事处罚，则终身不得从事网络安全管理和网络运营关键岗位的工作	甲如果违法情节轻微，尚不构成犯罪的，公安机关可以没收违法所得，处以拘留，可以并处罚款
496	多项选择题	我国涉及网络安全等级保护的法律法规和规范性文件包括（ ）。	《网络安全法》	《数据安全法》	《信息安全等级保护管理办法》	《信息安全等级保护商用密码管理办法》
497	多项选择题	《个人信息保护法》规定的个人信息处理者应当进行个人信息保护影响评估的情形包括（ ）。	向境外提供个人信息	利用个人信息进行自动化决策	委托第三方通过联邦计算等方式进行数据处理	借助差分隐私方法进行敏感个人信息处理
498	多项选择题	按照《个人信息保护法》，以下关于个人信息处理者在发生数据泄露时应履行通知义务的说法正确的是（ ）。	发生个人信息泄露的，应通知履行个人信息保护职责的部门和个人	通知应包括事件发生的原因和可能造成的后果	个人信息处理者如采取了有效的加密措施，能够有效避免信息泄露、篡改、丢失造成危害的，可以不通知个人	通知应包括个人信息处理者的联系方式和采取的补救措施
499	多项选择题	按照《个人信息保护法》，国家网信部门统筹协调有关部门推进的个人信息保护工作有（ ）。	制定个人信息保护各类具体规则、标准，如加密规范等	针对人脸识别、人工智能等新技术、新应用，制定专门的个人信息保护规则、标准	支持研发包括基于密码的安全电子身份认证技术，推进网络身份认证公共服务建设	推进个人信息保护社会化服务体系建设，支持有关机构开展个人信息保护评估、认证服务

500	多项选择题	以下可能违反《个人信息保护法》的情况有（）。	电子书APP以明文形式存储用户身份证号信息	出行类APP收集用户手机相册中的截图信息	电商类APP收集用户应用列表信息	天气类APP收集用户设备的精准位置（经纬度）信息
501	多项选择题	《个人信息保护法》要求个人信息处理者应当采取哪些确保个人信息安全的措施（　）。	数据分类	加密	去标识化	制定应急预案
502	多项选择题	按照《个人信息保护法》，以下关于加密和去标识化的说法正确的是（　）。	加密属于去标识化技术的一种	去标识化和加密属于不同的技术措施	去标识化可以和加密同时使用	对于敏感个人信息，去标识化后无必要再采用加密
503	多项选择题	按照《个人信息保护法》，以下关于加密和匿名化的说法正确的是（　）。	加密属于匿名化技术的一种	匿名化处理后的信息不属于个人信息	加密可以实现绝对的匿名化	只有通过不能复原的过程才能实现匿名化
504	多项选择题	在《个人信息保护法》中可以使用密码技术的场景有（　）。	收集个人信息	存储个人信息	个人信息出境	个人信息销毁
505	多项选择题	按照《个人信息保护法》，在个人信息出境前，应考虑的安全保护机制有（　）。	制定出境计划	开展出境评估	进行加密或采取去标识化措施	签订出境合同
506	多项选择题	按照《个人信息保护法》，以下属于个人信息的主体可以合理行使的对个人信息的权利有（　）。	要求复制一份自己的个人信息	拒绝填写非必填内容的个人资料	要求对所使用的加密技术进行说明	要求删除自己的个人信息并提供删除凭证
507	多项选择题	为确保个人信息处理活动符合法律、行政法规的规定，个人信息处理者应当根据个人信息的处理目的、处理方式、个人信息的种类以及对个人权益的影响、可能存在的安全风险等，采取下列哪些措施（　）。	制定内部管理制度和操作规程	对个人信息实行分类管理	采取相应的加密、去标识化等安全技术措施	制定并组织实施个人信息安全事件应急预案
508	多项选择题	按照《国家政务信息化项目建设管理办法》，网络安全监管部门应当依法加强对国家政务信息系统的安全监管，并指导监督项目建设单位落实网络安全审查制度要求，各部门应做到（　）。	严格遵守有关保密等法律法规规定	构建全方位、多层次、一致性的防护体系	按要求采用密码技术	定期开展密码应用安全性评估

509	多项选择题	按照《国家政务信息化项目建设管理办法》，国家政务信息化项目应向国家发展改革委备案。以下属于备案文件的有（　）。	运行维护经费和渠道情况	信息资源目录和共享开放情况	等级保护或者分级保护备案情况	密码应用方案和密码应用安全性评估报告
510	多项选择题	按照《国家政务信息化项目建设管理办法》，国家政务信息化项目的建设管理应当坚持的原则有（　）。	统筹规划	共建共享	业务协同	安全可靠
511	多项选择题	根据《国家政务信息化项目建设管理办法》，国家政务信息化项目建设单位在落实密码保障系统的要求时，应考虑（　）。	同步设计	同步规划	同步建设	同步运行
512	多项选择题	按照《国家政务信息化项目建设管理办法》，国家政务信息化项目验收的重要内容包括（　）。	软硬件产品的安全可靠情况	密码应用和安全审查情况	硬件设备能源利用效率情况	数据中心能源利用效率情况
513	多项选择题	按照《国家政务信息化项目建设管理办法》，国家政务信息化项目验收时，应提交的验收申请报告和材料包括以下（　）。	审计报告	安全风险评估报告	密码应用安全性评估报告	财务报告
514	多项选择题	按照《国家政务信息化项目建设管理办法》，以下属于项目建设单位不得新建、改建、扩建政务信息系统的情形是（　）。	重复采集数据	不符合密码应用要求	不符合网络安全要求	存在重大安全隐患
515	多项选择题	根据《国家政务信息化项目建设管理办法》，在构建政务信息系统防护体系时，应按要求采用密码技术，并定期开展密码应用安全性评估。整体安全架构要求是（　）。	全方位	多层次	立体化	一致性

516	多项选择题	中国在2020年关于“抓住数字机遇，共谋合作发展”的国际研讨会上提出《全球数据安全倡议》，指出在全球分工合作日益密切的背景下，确保信息技术产品和服务的供应链安全对于提升用户信心、保护数据安全、促进数字经济发展至关重要。加密技术作为保障供应链安全的关键技术之一，必然也面临同样的要求。为此，对待密码技术应当秉承（　）。	秉持发展和安全并重的原则	平衡处理密码技术进步与经济发展的关系	平衡处理密码技术进步与国家安全的关系	平衡处理密码技术进步与社会公共利益的关系
517	多项选择题	关于我国在2020年提出的《全球数据安全倡议》，说法正确的有（　）。	各国应积极维护全球信息技术产品和服务的供应链安全	各国应反对利用信息技术破坏他国关键基础设施或窃取重要数据的行为	各国应反对滥用信息技术从事针对他国的大规模监控行为	企业不得利用用户对产品依赖性谋取不正当利益
518	多项选择题	中国在2020年关于“抓住数字机遇，共谋合作发展”的国际研讨会上提出《全球数据安全倡议》，并倡议道：信息技术产品和服务供应企业不得控制或操纵用户系统和设备。根据我国《刑法》规定，对计算机信息系统实施非法控制将面临的处罚描述正确的是（　）。	情节严重的，处2年以下有期徒刑或拘役，并处或者单处罚金	情节严重的，处3年以下有期徒刑或者拘役，并处或者单处罚金	情节特别严重的，处3年以上7年以下有期徒刑，并处罚金	情节特别严重的，处2年以上5年以下有期徒刑，并处罚金
519	多项选择题	A公司系我国一家商用密码产品生产单位，2022年11月，其接到某国刑事司法调查机构的协助执法函，称该国一起刑事案件的犯罪嫌疑人将其生产的商用密码产品用于加密犯罪证据，要求A公司提供相关的密码算法和密钥数据，根据我国《数据安全法》，下列表述是正确的是（　）。	由于涉及司法调查，A公司有义务提供相关密码数据	如果相关密钥存储于境内，则A公司非经我国主管机关批准，不得提供	如果使用的是未公开的密码算法，则A公司非经我国主管机关批准，不得提供	A公司在任何情况下均不得提供商用密码算法和密钥
520	多项选择题	根据我国《数据安全法》，以下属于维护数据的完整性、保密性、可用性的内部风险管理机制的是（　）。	备份	加密	访问控制	渗透测试

521	多项选择题	根据我国《数据安全法》《数据出境安全评估办法》的规定，A单位对自身的商用密码技术数据申请重要数据出境安全评估，那么安全评估应当重点评估（　　）。	数据出境的目的、范围、方式等的合法性、正当性、必要性	出境数据的规模、范围、种类、敏感程度，数据出境可能对国家安全、公共利益、个人或者组织合法权益带来的风险	出境中和出境后遭到篡改、破坏、泄露、丢失、转移或者被非法获取、非法利用等的风险，以及数据安全是否能够得到充分有效保障	A单位与境外接收方拟订立的法律文件中是否充分约定了数据安全保护责任义务
522	多项选择题	按照《关键信息基础设施安全保护条例》的内容，某漏洞平台为增补现有的商用密码系统漏洞库，拟针对某商用密码科研单位实施大规模的渗透性测试，评估并发现潜在的漏洞风险。在实施渗透性测试之前，该商用密码科研单位被认定为关键信息基础设施运营者，则该漏洞平台为了能够合法地实施渗透性测试，需要（　　）。	经过国家网信部门批准	经过国务院公安部门批准	经过关键信息基础设施保护工作部门授权	经过该商用密码科研单位授权
523	多项选择题	按照《关键信息基础设施安全保护条例》，某商用密码服务机构的信息系统被依法认定为关键信息基础设施，在日常安全审计中，发现该信息系统近日来遭受持续的APT攻击，导致了大量商用密码业务数据的泄露，信息系统所在机构立即采取了相应的应急处置措施，但为了减少对于自身信誉的影响，选择不向主管部门报告，针对该行为，下列表述正确的是（　　）。	该机构已经采取了应急处置措施，不需要承担任何法律责任	该机构未向主管部门报告，应当给予警告	对该机构应当处10万元以上100万元以下罚款	对直接负责的主管人员应当处1万元以上10万元以下罚款

524	多项选择题	按照《关键信息基础设施安全保护条例》，关于关键信息基础设施中的密码管理，以下说法错误的是（　）。	关键信息基础设施中使用的密码属于普通密码	关键信息基础设施中使用密码产品或服务，一律先行经国家安全审查	国家密码管理局可以依法开展关键信息基础设施网络安全检查	对国家密码管理局依法开展的关键信息基础设施网络安全检查工作不予配合的，可以处以10万元以下罚款
525	多项选择题	按照《关键信息基础设施安全保护条例》，关键信息基础设施中的密码使用和管理还应当遵守的相关法律、行政法规有（　）。	《密码法》	《电子签名法》	《商用密码管理条例》	《网络安全等级保护基本要求》
526	多项选择题	按照《关键信息基础设施安全保护条例》，在开展关键信息基础设施网络安全检查工作中，保护工作部门和其他有关检查部门不应当（　）。	收取费用	要求购买指定密码产品	指定对检查风险进行整改的服务机构	将获取的信息用于非检查工作的其他用途
527	多项选择题	依据《信息安全等级保护管理办法》，某单位拟对其信息系统进行整改和升级，下列做法不正确的是（　）。	采用美国最先进的密码产品	使用本单位科研团队研发的先进密码产品	将密码的配备使用情况向国家密码管理机构备案	将信息系统中密码及密码设备的测评工作交由其他单位推荐的专家个人承担
528	多项选择题	关于《网络安全审查办法》，以下说法正确的是（　）。	网络安全审查涉及的对象包括所有网络运营者	国家网络安全审查工作机制的组建和成员机构包括国家密码管理局	网络安全审查办公室设在国家互联网信息办公室	网络安全审查涉及对所使用的密码产品或服务的安全性评估
529	多项选择题	关于《网络安全审查办法》涉及的密码产品或服务，以下说法正确的是（　）。	关键信息基础设施运营者采购密码产品或服务，应当了解其加密算法、密钥管理和协议等主要机制，预判采购后可能带来的国家安全风险	国家密码管理局如果认为可能影响国家安全的密码产品或服务需要进行网络安全审查的，由网络安全审查办公室按程序报批后审查	关键信息基础设施运营者应当强化密码产品和服务的供应链安全风险管理，预判采购后可能带来的国家安全风险	在进行国家安全审查时，向关键信息基础设施运营者或网络平台运营者提供密码产品或服务的供应商需要配合网络安全审查

530	多项选择题	某安全研究人员发现一款网络产品疑似存在密码漏洞，以下做法不符合《网络产品安全漏洞管理规定》的是（　）。	在网络产品提供者提供网络产品安全漏洞修补措施之前发布漏洞信息	披露网络、信息系统及其设备中存在该安全漏洞的细节	将漏洞信息与位于境外的安全社区共享	如发布网络产品安全漏洞的，应同步发布修补或者防范措施
531	多项选择题	关于网络产品的密码相关漏洞，以下说法正确的是（　）。	产品提供者发现其网络产品存在漏洞等风险，应采取补救措施	密码产品提供者应当在产品的质保期内持续提供安全维护	产品提供者可以通过委托网络安全服务机构对使用中的密码产品直接进行漏洞检测评估	密码漏洞不属于《网络安全法》规定的网络产品、服务漏洞
532	多项选择题	为了有效发现和修复商用密码产品中可能存在的安全漏洞，商用密码产品提供者可以（　）。	为使用该密码产品的用户提供安全维护服务	对发现并通报所提供的产品安全漏洞的组织或者个人给予奖励	对网络上疑似发布产品安全漏洞信息的行为保持密切关注	建立商用密码产品安全漏洞信息接收渠道并保持畅通
533	多项选择题	实施加密勒索攻击行为可能触犯的刑事罪名有（）。	非法侵入计算机信息系统罪	非法控制计算机信息系统罪	拒不履行信息网络安全管理义务罪	提供侵入、非法控制计算机信息系统程序、工具罪
534	多项选择题	与勒索攻击有关的刑事罪名有（　）。	非法侵入计算机信息系统罪	非法控制计算机信息系统罪	破坏计算机信息系统罪	侵犯公民个人信息罪
535	多项选择题	在刑事法律上对勒索攻击需要考虑的构成要件有（　）。	主观上存有故意	实施了侵入、非法控制计算机信息系统的行为	获取该计算机信息系统中或造成计算机信息系统不能正常运行等后果	实施的违法犯罪行为与危害后果之间有因果关系
536	多项选择题	行为人侵入国家核心密码和普通密码研发系统，可能构成的刑事罪名是（　）。	非法侵入计算机信息系统罪	非法利用信息网络罪	非法获取国家秘密罪	破坏计算机信息系统罪
537	多项选择题	某网络运营者未履行对用户敏感个人信息的加密存储义务，如导致以下哪些后果之一的，经监管部门责令采取改正措施而拒不改正，则可能构成拒不履行信息网络安全管理义务罪（　）。	致使用户无法登录账户，需要重置的	致使用户信息泄露，造成严重后果的	致使刑事案件证据灭失，情节严重的	致使用户个人信息错误，需要更正的

538	多项选择题	我国《刑法》中与出口国家禁止出口的密码管制物项或者未经许可出口密码管制物项有关的罪名有（　）。	走私国家禁止进出口的货物、物品罪	非法经营罪	泄露国家秘密罪	逃避商检罪
539	多项选择题	按照商务部《中国禁止出口限制出口技术目录》，以下属于禁止出口的密码的技术或产品包括（　）。	涉及保密原理、方案及线路设计技术的卫星数据加密技术	涉及加密与解密软件、硬件的卫星数据加密技术	卫星及其运载无线电遥控遥测编码和加密技术	北斗卫星导航系统信息传输加密技术
540	多项选择题	按照商务部《中国禁止出口限制出口技术目录》，以下属于限制出口的密码的技术或产品包括（　）。	高速密码算法的密码芯片设计和实现技术	量子密码技术	密码漏洞发现和挖掘技术	片上密码芯片（SOC）设计与实现技术
541	多项选择题	按照商务部、科技部《中国禁止进口限制进口技术目录》，以下属于限制进口的密码的技术或产品包括（　）。	安全强度不高于64位加密算法的加密技术	安全强度不高于128位加密算法的加密技术	安全强度高于256位加密算法的加密技术	安全强度高于1024位加密算法的加密技术
542	多项选择题	按照商务部、科技部《中国禁止进口限制进口技术目录》，是否限制进口时考虑的因素包括（）。	进口后将对国家安全、社会公共利益造成的不利影响	进口后对生态环境产生的不利影响	依照法律、行政法规的规定需要限制进口	根据我国缔结或者参加的国际公约、国际协定的规定需要限制进口
543	判断题	根据《网络安全法》，网络运营者应对所有数据采取加密措施。	正确	错误		
544	判断题	根据《网络安全法》，网络运营者应当采取数据分类、重要数据备份和加密等措施，以履行网络安全保护义务。	正确	错误		
545	判断题	根据《网络安全法》，窃取他人加密保护的信息，非法侵入他人的密码保障系统、并根据《密码法》规定受到处罚的人员，三年内不得从事网络安全管理和网络运营关键岗位的工作。	正确	错误		

546	判断题	按照《关键信息基础设施安全保护条例》，关键信息基础设施运营者对密码管理部门依法开展的关键信息基础设施网络安全检查工作应当予以配合。	正确	错误		
547	判断题	按照《关键信息基础设施安全保护条例》，关键信息基础设施运营者如果对密码管理等有关部门依法开展的检查工作不予配合，且由有关主管部门责令改正后拒不改正的，将被处1万元以上10万元以下罚款。	正确	错误		
548	判断题	按照《关键信息基础设施安全保护条例》，关键信息基础设施中的密码使用和管理，应当遵守《密码法》等相关法律、行政法规的规定。	正确	错误		
549	判断题	根据《国家政务信息化项目建设管理办法》，除国家发展改革委审批或者核报国务院审批的外，其他有关部门自行审批新建、改建、扩建，以及通过政府购买服务方式产生的国家政务信息化项目，应当按规定履行审批程序并向国家发展改革委备案。	正确	错误		
550	判断题	根据《国家政务信息化项目建设管理办法》，国家政务信息化项目建设单位应当同步规划、同步建设、同步运行密码保障系统并定期进行评估。	正确	错误		
551	判断题	根据《国家政务信息化项目建设管理办法》，国家政务信息化项目验收的内容中，不包括安全风险评估报告。	正确	错误		
552	判断题	根据《国家政务信息化项目建设管理办法》，国家政务信息化项目建设单位提交验收申请报告时，应当一并附上密码应用安全性评估报告。	正确	错误		

553	判断题	根据《国家政务信息化项目建设管理办法》，对于不符合密码应用和网络安全要求，或者存在重大安全隐患的政务信息系统，可以通过安排运行维护经费进行整改。	正确	错误		
554	判断题	根据《国家政务信息化项目建设管理办法》，国务院办公厅、国家发展改革委、财政部、中央网信办会同有关部门对国家政务信息化项目中的密码应用、网络安全等情况实施监督管理。	正确	错误		
555	判断题	根据《国家政务信息化项目建设管理办法》，各部门应当定期开展密码应用安全性评估，确保政务信息系统运行安全和政务信息资源共享交换的数据安全。	正确	错误		
556	判断题	根据《信息安全等级保护管理办法》,等级保护工作中有关密码工作的监督、检查、指导由国家密码管理部门负责。	正确	错误		
557	判断题	根据《信息安全等级保护管理办法》,国家密码管理部门对信息安全等级保护的密码实行分类分级管理。	正确	错误		
558	判断题	根据《信息安全等级保护管理办法》,信息系统运营、使用单位采用密码进行等级保护的，应当遵照《信息安全等级保护密码管理办法》、《信息安全等级保护商用密码技术要求》等密码管理规定和相关标准。	正确	错误		
559	判断题	根据《信息安全等级保护管理办法》,信息系统安全等级保护中密码的配备、使用和管理等，应当严格执行国家密码管理的有关规定。	正确	错误		
560	判断题	根据《信息安全等级保护管理办法》,采用密码对涉及国家秘密的信息和信息系统进行保护的，应经报保密行政管理部门审批。	正确	错误		

561	判断题	根据《信息安全等级保护管理办法》,运用密码技术对信息系统进行系统等级保护建设和整改的，未经批准不得采用含有加密功能的进口信息技术产品。	正确	错误		
562	判断题	根据《信息安全等级保护管理办法》,未经国家密码管理局认可的测评机构，不得对信息系统中的密码及密码设备进行评测。	正确	错误		
563	判断题	根据《信息安全等级保护管理办法》,各级密码管理部门对信息系统等级保护工作中密码使用和管理的情况每年至少进行一次检查和测评。	正确	错误		
564	判断题	根据《信息安全等级保护管理办法》,在等级保护工作的监督检查过程中，发现未达到密码相关标准要求的，应当按照国家密码管理的相关规定进行处置。	正确	错误		
565	判断题	根据《信息安全等级保护管理办法》,第三级以上信息系统运营单位违反密码管理规定的，由公安机关、国家保密工作部门和国家密码工作管理部门按照职责分工责令其限期改正。	正确	错误		
566	判断题	根据《个人信息保护法》，个人信息处理者应当采取措施确保个人信息处理活动符合法律、行政法规的规定，并防止未经授权的访问以及个人信息泄露、篡改、丢失,措施中包括相应的加密、去标识化等安全技术措施。	正确	错误		
567	单项选择题	我国金融信息系统、第二代居民身份证管理系统、国家电力信息系统、社会保障信息系统、全国中小学学籍管理系统中，都应用（　）技术构建了密码保障体系。	核心密码	普通密码	商用密码	核心密码和普通密码

568	单项选择题	商用密码从业单位开展商用密码活动，应当符合该从业单位公开标准的技术要求，对此下列说法正确的是（ ）。	企业生产的商用密码产品如果执行团体标准，则不需要公开相应标准编号	企业生产的商用密码产品如果执行的标准是本企业制定的企业标准，只需要公开标准名称	公开指标的类别和内容由企业根据自身特点自主确定，可以不公开私钥	企业应当公开其提供的密码产品的设计细节
569	单项选择题	以下密码算法没有成为国际标准的是（ ）。	SM1分组密码算法	SM4分组密码算法	SM9数字签名算法	ZUC密码算法
570	单项选择题	近些年，我国建立和完善商用密码标准体系，商用密码标准取得较大进展，对此下列说法正确的是（ ）。	我国已经发布了商用密码的强制性国家标准	我国商用密码现行国家标准均为推荐性的	商用密码行业标准不能上升为国家标准	我国有强制性的商用密码行业标准
571	单项选择题	密码的加密保护功能用于保证（ ）。	信息的机密性	信息的真实性	数据的完整性	行为的不可否认性
572	单项选择题	密码在网络空间中身份识别、安全隔离、信息加密、完整性保护和抗抵赖性等方面具有不可替代的重要作用，可实现信息的（ ）、（ ）、数据的（ ）和行为的（ ）。	机密性、真实性、完整性、不可否认性	秘密性、确定性、完整性、不可替代性	机密性、安全性、统一性、不可抵赖性	秘密性、有效性、统一性、不可逆转性
573	单项选择题	商用密码服务是指基于商用密码专业技术、技能和设施，为他人提供集成、运营、监理等商用密码（ ）的活动。	支持和保障	进出口	产品生产	产品销售
574	单项选择题	关于商用密码应用安全性评估的原则，以下表述错误的是（ ）。	商用密码应用安全性评估实施分类分级管理	新建的重要领域网络和信息系统，应当在规划、建设、运行三个阶段开展评估	已建成的重要领域网络和信息系统不再需要开展评估	商用密码应用安全性评估的关键点是网络和信息系统密码应用的合规性、正确性和有效性
575	单项选择题	截至2023年6月1日，国家密码管理部门已经发布（ ）期商用密码应用安全性评估试点机构目录。	1	2	3	4

576	单项选择题	截至2023年6月1日，根据国家密码管理局发布的相关文件、通知，我国有商用密码应用安全性评估试点机构资格的机构一共有（　）。	24家	36家	73家	60家
577	单项选择题	《政务信息系统密码应用与安全性评估工作指南》（2020版）的适用对象是（　）。	非涉密的国家政务信息系统建设单位和使用单位	政务信息系统集成单位	商用密码应用安全性评估机构	以上都是
578	单项选择题	《政务信息系统密码应用与安全性评估工作指南》（2020版）制定的依据不包括（　）。	《国家政务信息化项目建设管理办法》	《商用密码应用安全性评估管理办法（试行）》	《电子政务电子认证服务业务规则规范》	《中华人民共和国密码法》
579	单项选择题	根据《政务信息系统密码应用与安全性评估工作指南》（2020版），关于政务信息系统密码应用与安全性评估实施过程的表述，错误的是（　）。	密码应用方案通过密评是项目立项的必要条件	建设阶段涉及密码应用方案调整优化的，应委托密评机构再次对调整后的密码应用方案进行确认	系统通过密评是项目验收的必要条件	初次未通过密评的政务信息系统，不得通过项目验收。
580	单项选择题	根据《政务信息系统密码应用与安全性评估工作指南》（2020版），在政务信息系统运行阶段，关于密码应用与安全性评估的要求，错误的是（　）。	在政务信息系统运行阶段，项目使用单位定期委托密评机构对系统开展密评	网络安全保护等级第三级及以上的政务信息系统，每年至少密评一次	密评可与关键信息基础设施网络安全审查、网络安全等级测评等工作统筹考虑、协调开展。	运行后的政务信息系统密评未通过的，项目使用单位按要求对系统进行整改后再次开展密评。
581	单项选择题	根据《政务信息系统密码应用与安全性评估工作指南》（2020版），关于密评机构对政务信息系统开展密评工作的表述，正确的是（　）。	密评机构负责对政务信息系统的密码应用方案进行密评	密评机构负责对政务信息系统开展密评	密评机构对政务信息系统开展密评时，应从总体要求、物理和环境安全、网络和通信安全、设备和计算安全、应用和数据安全、密钥管理、安全管理等方面开展评估	以上都对

582	单项选择题	根据《政务信息系统密码应用与安全性评估工作指南》（2020版），密评机构对政务信息系统开展密评时，需依据的标准规范、指导性文件及管理要求是（　）。	《商用密码应用安全性评估管理办法（试行）》	《信息系统密码测评要求（试行）》	《商用密码应用安全性评估测评过程指南（试行）》	以上都是
583	多项选择题	密码行业标准化技术委员会的主要职责包括（　）。	提出密码行业标准规划和年度标准制定、修订计划的建议	组织密码行业标准的编写、审查、复审等工作	组织密码领域的国家和行业标准的宣传贯彻，推荐密码领域标准化成果申报科技进步奖励	受国家标准化管理委员会委托，对相关国际标准文件进行表决、审查我国提案
584	多项选择题	根据《政务信息系统密码应用与安全性评估工作指南》（2020版），某单位拟建设政务信息系统，下列建设环节中符合法律要求的是（　）。	密码应用方案应当通过密评	密码应用方案一旦通过密评须严格遵守，不得调整	系统建设完成后，必须对系统开展密评	系统通过密评是项目验收的必要条件
585	多项选择题	按照《政务信息系统密码应用与安全性评估工作指南》（2020版）的内容，政务信息系统的建设单位，需要对政务信息系统进行保护，其中包括建立安全的密钥管理方案、采取有效的安全管理措施、采用密码技术措施等，其中密码技术措施包括（　）。	物理和环境安全	网络和通信安全	设备和计算安全	应用和数据安全
586	多项选择题	根据《政务信息系统密码应用与安全性评估工作指南》（2020版），政务信息系统的安全管理措施包括（　）。	制度	人员	实施	应急
587	多项选择题	按照《政务信息系统密码应用与安全性评估工作指南》（2020版），在政务信息系统中，密评机构的职责主要包括（　）。	对政务信息系统的密码应用方案进行密评	对单位人员进行审查	对政务信息运行流程进行评估	对政 务信息系统开展密评
588	多项选择题	按照人社部《职业分类大典》，以下与密码技术直接相关的职业是（　）。	密码技术应用员	密码管理员	密码工程技术人员	密码分析员

589	判断题	商用密码在我们生活中无处不在，例如我们的二代居民身份证也使用了商用密码。	正确	错误		
590	判断题	我国商用密码行业标准的代号是GM。	正确	错误		
591	判断题	我国密码行业的标准化组织是国家密码管理局。	正确	错误		
592	判断题	在《政务信息系统密码应用与安全性评估工作指南》（2020版）中，编制政务信息系统密码应用方案应遵循总体性原则、完备性原则及适用性原则。	正确	错误		
593	判断题	根据《政务信息系统密码应用与安全性评估工作指南》（2020版），在政务信息系统建设阶段，系统通过密评并不是项目验收的必要条件。	正确	错误		
594	判断题	根据《政务信息系统密码应用与安全性评估工作指南》（2020版），未经检测认证的密钥管理方案技术实现可向国家密码管理部门进行备案。	正确	错误		
595	多项选择题	下面关于密码学的基本概念说法正确的是（ ）。	原始的消息称为明文	经过加密的消息称为密文	用来传输消息的通道称为信道	消息的接发送者称为信宿
596	单项选择题	根据Kerckhoffs原则，密码系统的安全性主要依赖于（ ）。	密钥	加密算法	解密算法	通信双方
597	多项选择题	在分组密码设计中用到扩散和混淆的理论。理想的扩散是（ ）。	明文的一位只影响密文对应的一位	让密文中的每一位受明文中每一位的影响	让明文中的每一位影响密文中的所有位。	一位明文影响对应位置的密文和后续密文
598	多项选择题	在分组密码设计中用到扩散和混淆的理论。理想的混淆是（ ）。	使密文和密钥之间的统计关系变得尽可能复杂	使得对手即使获得了关于密文的一些统计特性，也无法推测密钥	使用复杂的非线性代换	让密文中的每一位受明文中每一位的影响

599	单项选择题	2000年10月，美国NIST宣布（ ）算法作为新的高级加密标准AES。	Rijndael	RC6	SERPENT	Twofish
600	单项选择题	根据密码分析者所掌握的分析资料的不同，密码分析一般可为四类：唯密文攻击、已知明文攻击、选择明文攻击、选择密文攻击，其中（ ）是在公开的网络中能获得的最现实的能力。	唯密文攻击	已知明文攻击	选择明文攻击	选择密文攻击
601	单项选择题	密码学理论研究通常包括哪两个分支（ ）。	对称加密与非对称加密	密码编码学与密码分析学	序列算法与分组算法	DES和 RSA
602	多项选择题	下列我国商密算法中，被纳入国际标准化组织ISO/IEC的包括（ ）。	SM2数字签名算法	SM3密码杂凑算法	SM4分组密码算法	祖冲之密码算法
603	单项选择题	以下选项中各种加密算法中不属于对称加密算法的是（ ）。	DES算法	SM4算法	AES算法	Diffie-Hellman算法
604	单项选择题	以下选项中各种加密算法中属于非对称加密算法的是（ ）。	DES算法	Caesar密码	Vigenere密码	RSA算法
605	单项选择题	对RSA算法的描述正确的是（ ）。	RSA算法是对称密钥算法	RSA算法是公钥算法	RSA算法是一种流密码	RSA算法是杂凑函数算法
606	单项选择题	杂凑函数不可直接应用于（ ）。	数字签名	安全存储口令	加解密	数字指纹
607	单项选择题	商用密码可以保护的范畴为（ ）。	绝密级以下（含绝密级）的国家秘密	机密级以下（含机密级）的国家秘密	秘密级以下（含秘密级）的国家秘密	不属于国家秘密的信息
608	单项选择题	一个完整的密码体制，不包括（ ）要素。	明文空间	密文空间	密钥空间	数字签名
609	单项选择题	以下不是SM2算法的应用场景的有（ ）。	生成随机数	协商密钥	加密数据	数字签名
610	单项选择题	一个序列密码具有很高的安全强度主要取决于（ ）。	密钥流生成器的设计	初始向量长度	明文长度	加密算法
611	单项选择题	以下哪不属于密码学的具体应用的是（ ）。	人脸识别技术	消息认证，确保信息完整性	加密技术，保护传输信息	进行身份认证
612	单项选择题	（ ）原则上能保证只有发送方与接受方能访问消息内容。	保密性	鉴别	完整性	数字签名
613	单项选择题	存储、处理国家秘密的计算机信息系统按照涉密程度实行（ ）。	专人保护	分级保护	重点保护	特殊保护

614	单项选择题	目前公开密钥密码主要用来进行数字签名，或用于保护传统密码的密钥，而不主要用于数据加密，主要因为（ ）。	公钥密码的密钥太短	公钥密码的效率比较低	公钥密码的安全性不好	公钥密码抗攻击性比较差
615	单项选择题	如果密钥序列的产生独立于明文消息和密文消息，那么此类序列密码称为（ ）。	同步序列密码	非同步序列密码	自同步序列密码	移位序列密码
616	单项选择题	序列密码的安全性取决于（ ）的安全性。	移位寄存器	S盒	密钥流	生成多项式
617	单项选择题	（ ）密码体制，其原理是加密密钥和解密密钥分离。这样，一个具体用户就可以将自己设计的加密密钥和算法公诸于众，而只保密解密密钥。	对称	私钥	代换	公钥
618	单项选择题	下列选项中不属于公钥密码体制的是（ ）。	ECC	RSA	ELGamal	DES
619	单项选择题	设杂凑函数的输出长度为 n bit，则安全的杂凑函数寻找碰撞的复杂度应该为（ ）。	O(P(n))	O(2^n)	O(2^{n/2})	O(n)
620	单项选择题	原始的Diffie-Hellman密钥交换协议易受（ ）。	中间人攻击	选择密文攻击	已知明文攻击	被动攻击
621	单项选择题	多变量公钥密码的安全性基础是基于（ ）的困难性。	求解有限域上随机生成的多变量非线性多项式方程组	大整数分解	任意线性码的译码问题	最小整数解问题
622	单项选择题	使用有效资源对一个密码系统进行分析而未被破译，则该密码是（ ）。	计算上安全	不安全	无条件安全	不可破译
623	单项选择题	数字签名能够提供，而消息认证码无法提供的安全属性是（ ）。	机密性	认证	随机性	不可否认性
624	单项选择题	下列选项不是密码系统基本部分组成的是（ ）。	明文空间	密码算法	初始化	密钥
625	多项选择题	下面属于杂凑函数算法的是（ ）。	MD5	SHA-1	SHA-2	ECC
626	多项选择题	密码技术能提供的安全服务有（ ）。	加密	机密性	完整性	可靠性

627	多项选择题	我国涉密人员分为（ ）。	核心涉密人员	非常重要涉密人员	重要涉密人员	一般涉密人员
628	多项选择题	一个完整的密码体制，包括以下（ ）要素。	明文空间	密文空间	数字签名	密钥空间
629	多项选择题	以下攻击方式属于基本攻击类型的是（ ）。	选择明文攻击	已知明文攻击	选择密文攻击	唯密文攻击
630	多项选择题	1976年，提出公钥密码学系统的学者是（ ）。	Diffie	Shamir	Hellman	Hill
631	单项选择题	关于对称加密和非对称加密，以下说法正确的是（ ）。	对称加密的安全性较高	对称加密一定比非对称加密的安全性高	对称加密的效率较高	非对称加密的效率较高
632	多项选择题	下列攻击行式中，属于主动攻击的是（ ）。	伪造	篡改	中断	监听
633	多项选择题	密码学的基本属性包括哪些（ ）。	信息的机密性	信息的真实性	数据的完整性	行为的不可否认性
634	多项选择题	古典密码主要包括（ ）等形式。	置换密码	分组密码	转轮密码	代换密码
635	多项选择题	下列选项属于针对密码协议的常见攻击方法的是（ ）。	重放攻击	并行会话攻击	中间人攻击	预言者会话攻击
636	判断题	量子密码与传统的密码系统不同，它主要依赖物理学的相关技术。	正确	错误		
637	判断题	量子密钥分发是现阶段量子保密通信最主要的应用方式。	正确	错误		
638	判断题	一般来说，密码学中可能的攻击方式可以归纳为三种攻击策略:根据密码系统所依据的基本原理中存在的漏洞进行攻击的策略；根据密码分析者所获取的有效信息进行攻击的策略；根据密码系统结构上的漏洞进行攻击的策略。	正确	错误		
639	判断题	在密码学中，需要被变换的原消息被称为密文。	正确	错误		
640	判断题	古典密码体制中，移位密码属于置换密码。	正确	错误		
641	判断题	机密信息是重要的国家秘密，泄露会使国家安全和利益遭受严重的损害。	正确	错误		

642	判断题	多表代换密码是以一系列代换表一次对明文消息的字母序列进行代换的加密方法。	正确	错误		
643	判断题	移位加密是一种无密钥的加密方式。	正确	错误		
644	判断题	完善保密加密最初是由香农（Shannon）提出并进行研究的。	正确	错误		
645	判断题	简单来说，差分分析就是系统地研究明文中的一个细小变化是如何影响密文的。	正确	错误		
646	判断题	在置换密码算法中，密文所包含的字符集与明文的字符集是相同的。	正确	错误		
647	判断题	商用密码用于保护属于国家秘密的信息。	正确	错误		
648	判断题	“一次一密”的随机密码序列体制在理论上是不可破译的。	正确	错误		
649	判断题	我国国家密码管理局公布的第一个商用密码算法为ZUC-128算法。	正确	错误		
650	判断题	代换密码与置换密码是同一种密码体制。	正确	错误		
651	判断题	一个密码系统是无条件安全又称为可证明安全。	正确	错误		
652	判断题	现代密码的安全性不应该依赖于密码算法的保密性，而应该依赖密钥的保密性。	正确	错误		
653	多项选择题	以下关于对称密钥加密的说法正确的是( )。	对称加密算法的密钥易于管理	加解密双方使用同样的密钥	DES算法属于对称加密算法	相对于非对称加密算法，加解密处理速度比较快
654	多项选择题	相对于对称加密算法，非对称密钥加密算法( )。	加密数据的速率较低	更适合于对长数据的加解密处理	在大规模节点网络环境下，密钥分配较为方便	加密和解密的密钥不同
655	多项选择题	密码分析是研究密码体制的破译问题，根据密码分析者所获得的数据资源，可以将密码攻击分为（ ）。	唯密文攻击	已知明文攻击	选择明文攻击	选择密文攻击

656	多项选择题	常见的后量子密码（或抗量子密码）技术的研究领域都包含哪些包括（ ）。	基于编码后量子密码	基于多变量后量子密码	基于格后量子密码	基于杂凑算法后量子密码
657	多项选择题	基于格理论密码是重要的后量子密码技术之一。下述属于格理论困难问题的是（ ）。	最短向量问题(Shortest Vector Problem, SVP)	最近向量问题,Closest Vector Problem	容错学习(Learning With Errors, LWE)	最小整数解(Small Interger Solution)
658	多项选择题	下述关于密码学论述的观点正确的是（ ）。	密码学的属性包括机密性、完整性、真实性、不可否认性	密码学的两大分支是密码编码学和密码分析学	密码学中存在一次一密的密码体制，理论上它是绝对安全的	密码技术并不是提供安全的唯一手段
659	多项选择题	属于密码在信息安全领域的具体应用的是（ ）。	生成所有网络协议	消息鉴别，确保信息完整性和真实性	加密保护，保护传输信息的机密性	身份鉴别
660	多项选择题	密码学发展的三个阶段（ ）。	代换、置换密码	古典密码	近代密码	现代密码
661	单项选择题	量子密钥分发（QKD）技术采用（ ）作为信息载体，经由量子通道在合法的用户之间传送密钥。	数据	电流	量子态	文本
662	单项选择题	置换（permutation）密码是把明文中的各字符（ ）得到密文的一种密码体制。	位置次序重新排列	替换为其他字符	增加其他字符	减少其他字符
663	单项选择题	代换（substitution）密码是把明文中的各字符（ ）得到密文的一种密码体制。	位置次序重新排列	替换为其他字符	增加其他字符	减少其他字符
664	单项选择题	一个密码系统由明文、密文、加密算法、解密算法和密钥5部分组成，而其安全性主要是由（ ）的保密性决定的。	加密算法	解密算法	加解密算法	密钥
665	单项选择题	对于一个密码系统，若利用已有的最好计算方法，破译它的所需要的代价超出了破译者的破译能力（如时间、空间、资金等资源），那么该密码系统的安全性是（ ）。	无条件安全	计算安全	可证明安全	理论安全
666	单项选择题	SM2算法是（ ）密码算法。	序列密码	对称密码算法	公钥密码	密码杂凑函数

667	多项选择题	我国SM2公钥密码算法包含的3个算法是（ ）。	数字签名算法	密钥封装算法	密钥交换协议	公钥加密解密算法
668	单项选择题	不可否认性一般使用（ ）密码技术实现。	对称加密	MAC码	数字信封	数字签名
669	单项选择题	以下哪种情况可以实现对消息完整性的认证，也提供消息源真实性鉴别（ ）。	对消息进行SM3杂凑计算，将消息和杂凑值一并发送给接受者	对消息进行SM4-CTR计算，将密文发送给接受者	对消息进行SM2签名计算，将消息和签名一并发送给接受者	对消息进行SM3杂凑计算，将消息发送给接受者，并通过可靠的方式将消息的摘要离线发送接受者，保证摘要值无法被攻击者篡改
670	单项选择题	以下关于完整性保护实现机制描述正确的是（ ）。	开发人员使用SM4-CBC算法对不定长消息计算MAC值。	开发人员使用SM3-HMAC对消息计算MAC值，HMAC计算过程中使用了3次杂凑计算。	基于对称密码或者杂凑算法的MAC机制能够确保接收者接收消息之前的消息完整性，但是不能防止接收者对消息的伪造。	当采用数字签名方式时，验证方仅使用签名值和签名私钥相应的公钥证书即可完成签名验证。
671	单项选择题	查看数据库发现一段密文长度为256比特，则可以确定使用的密码算法为（ ）。	SM2	SM3	SM4	无法判断
672	多项选择题	GB/T 15852《信息技术 安全技术 消息鉴别码》标准中定义的消息鉴别码可以基于（ ）机制实现。	分组密码	泛杂凑函数	非对称密码	专用杂凑函数
673	多项选择题	量子计算中的Shor算法，对哪些传统密码算法安全性产生较大威胁（ ）。	RSA	DSA	AES	SM3
674	单项选择题	以下哪个算法在量子攻击下不再安全（ ）。	AES-256	SHA-512	RSA-15360	ZUC-256

675	多项选择题	主动攻击者可以通过将事先保存的正确 MAC 值不断重放来发动攻击。以下哪几种方法可以防御重放攻击（ ）。	每次都对发送的消息赋予一个递增的编号（ 序号 ），并且在计算 MAC 值时将序号也包含在消息中	在发送消息时包含当前的时间，如果收到以前的消息，即便 MAC 值正确也将其当做错误的消息来处理	在通信之前，接收者先向发送者发送一个一次性的随机数，发送者在消息中包含这个 nonce 并计算 MAC 值	每次都对发送的消息携带发送者的唯一身份标识，并且在计算 MAC 值时该标识也包含在消息中
676	判断题	在可证明安全理论中，不可预测远远强于伪随机性。	正确	错误		
677	判断题	ZUC序列密码算法主要用于加密手机终端与基站之间的传输的语音和数据。	正确	错误		
678	单项选择题	国家支持社会团体、企业利用自主创新技术制定（ ）国家标准、行业标准相关技术要求的商用密码团体标准、企业标准。	低于	等于	高于	相当于
679	单项选择题	在密码的实际应用中，通常使用下列哪种方法来实现不可否认性（ ）。	加密	数字签名	时间戳	数字指纹
680	单项选择题	IDEA加密算法是一种（ ）。	分组密码	序列密码	置换密码	代替密码
681	单项选择题	ECC（Ellipse Curve Ctyptography）是一种基于椭圆曲线密码体制，属于哪一类密码体制（ ）。	分组密码	对称密码	序列密码	非对称密码
682	单项选择题	在1977年，美国国家标准局将（ ）设计的的Tuchman-Meyer方案确定为数据加密标准，即DES（Data Encryption Standard）。	苹果公司	谷歌公司	IBM公司	惠普公司
683	单项选择题	在密码体制的分类中，根据密钥的特点，可将密码体制分为对称和非对称两种，如（ ）。	RSA等是对称密码体制，Vernam密码、ElGamal等是非对称密码体制	ElGamal等是对称密码体制，Vernam密码、AES等是非对称密码体制	Vernam、AES等是对称密码体制，RSA密码、ElGamal等是非对称密码体制	Vernam、ElGamal等是对称密码体制，RSA密码、AES等是非对称密码体制
684	多项选择题	以下属于现代密码学范畴的是（ ）。	DES	Vigenere密码	Caesar密码	RSA

685	多项选择题	以下属于非对称密码体制的有（ ）。	AES	Vigenere	ElGamal	RSA
686	多项选择题	以下属于典型的古典密码体制的有（ ）。	Caesar密码	Vigenere密码	RSA算法	AES算法
687	多项选择题	代换（substitution）密码分为以下哪些类型（ ）。	单表代换密码	多表代换密码	循环移位密码	置换密码
688	多项选择题	在我国商用密码中，密码系统通常由明文、密文、加密算法、解密算法和密钥五部分组成，其中可以公开的部分是（ ）。	加密算法	解密算法	密文	密钥
689	单项选择题	维吉利亚密码是古典密码体制比较有代表性的一种密码，其采用的加密变换方法的是（ ）。	置换	单表代换	多表代换	仿射变换
690	多项选择题	以下关于置换（permutation）密码说法正确的是（ ）。	置换密码又称为换位密码	置换密码分为列置换密码、行置换密码	周期置换密码是将明文串按固定长度分组，然后对每组中的子串按某个置换重新排列位置从而得到密文	著名的古典凯撒密码是置换密码
691	单项选择题	我国商用密码杂凑函数SM3迭代结构是（ ）。	平衡Fesitel网络结构	非平衡Fesitel网络结构	SP结构	MD结构
692	多项选择题	以下加密算法中不属于古典加密算法的是（ ）。	Caesar密码	DES算法	IDEA算法	Differ-Hellman算法
693	多项选择题	与量子密码相对应，经典密码学包括（ ）。	密码编码学	密码分析学	后（抗）量子密码学	量子密码
694	判断题	仿射密码的加密算法是线性变换。	正确	错误		
695	判断题	置换（permutation）密码采用线性变换对明文进行处理。	正确	错误		
696	判断题	在置换（permutation）密码算法中，密文所包含的字符集与明文的字符集是相同的。	正确	错误		
697	判断题	古典Vigenere密码是一个单表代换密码。	正确	错误		

698	判断题	多表代换密码是以多个不同的代换表对明文消息的字母序列进代换的密码。	正确	错误		
699	判断题	周期置换密码是将明文串按固定长度分组，然后对每个分组中的子串按某个置换重新排列组合从而得到密文。	正确	错误		
700	单项选择题	Hill密码是重要古典密码之一，其加密的核心思想的是（ ）。	线性变换	非线性变换	循环移位	移位
701	单项选择题	著名的 Kerckhoff 原则是指（ ）。	系统的保密性不但依赖于对加密体制或算法的保密，而且依赖于密钥	系统的保密性不依赖于对加密体制或算法的保密，而依赖于密钥	系统的保密性既不依赖于对加密体制或算法的保密，也不依赖于密钥	系统的保密性只与其使用的安全算法的复杂性有关
702	单项选择题	下面哪种密码可以抵抗频率分析攻击（ ）。	置换密码	仿射密码	多表代换密码	凯撒密码
703	单项选择题	《保密系统的通信理论》这篇论文把密码学置于坚实的数学基础之上，标志着密码学作为一门学科的形成，该论文的作者是（ ）。	香农	图灵	布尔	迪菲
704	单项选择题	从密码学的角度来看，凯撒密码属于（ ）加密。	单字母表替换	单字母表混淆	多字母表替换	多字母表混淆
705	单项选择题	1949年香农发表的学术论文（ ）标志着现代密码学的真正开始。	《密码学的新方向》	《保密系统的通信理论》	《战后密码学的发展方向》	《公钥密码学理论》
706	单项选择题	1976年，Diffie和Hellman发表了一篇著名论文（），提出了著名的公钥密码体制的思想。	《密码学的新方向》	《保密系统的通信理论》	《战后密码学的发展方向》	《公钥密码学理论》
707	多项选择题	评价密码系统安全性主要有以下哪些方法（ ）。	计算安全性	无条件安全性	加密安全性	可证明安全性
708	多项选择题	对分组密码分析，时间-存储权衡攻击是由以下哪些方法混合而成（ ）。	强力攻击	字典攻击	查表攻击	穷尽密钥搜索攻击
709	多项选择题	作为分组密码的分析方法，多线性逼近方法是由以下哪些作者提出的（ ）。	Kaliski	Shamir	Rivest	Robshaw
710	多项选择题	下列可以预防重放攻击的是（ ）。	时间戳	nonce	序号	明文填充

711	多项选择题	下列哪些参数决定了穷举攻击所消耗的时间（）。	密钥空间	密钥长度	主机运算速度	主机显存容量
712	多项选择题	下列属于NP问题的是（ ）。	背包问题	整数分解问题	矩阵覆盖问题	陪集重量问题
713	多项选择题	下列密码分析方法属于已知明文攻击的是（ ）。	最佳放射逼近分析方法	线性密码分析方法	分别征服分析方法	时间-存储权衡攻击
714	多项选择题	一般而言，密码体制可以对信息提供的主要功能有（ ）。	机密性	真实性	完整性	不可否认性
715	单项选择题	我国SM2算法系列标准中，不包含对于以下哪种密码应用的使用规范。	公钥加密	数字签名	密钥交换	身份认证
716	单项选择题	以下说法正确的是（ ）。	SM4的密钥长度为128比特，那么用暴力破解找到正确密钥需要平均尝试约2的127次方	通过PBKDF（口令为16位随机数字）生成的128比特密钥的密钥空间等同于SM4算法密钥空间	MQV密钥交换协议无法抵抗中间人攻击，但SM2密钥交换协议可以抵抗该攻击	AES-256-CBC加密模式的IV值要求是随机值且保密
717	单项选择题	后量子密码是指（ ）。	基于量子原理设计的密码算法	能够攻破量子计算机的密码	能够抵抗量子计算机攻击的密码	具有量子不确定特性的密码算法
718	单项选择题	一个安全的密码杂凑函数需要能够抵抗生日攻击等强抗碰撞性攻击。生日攻击即：在随机抽出的N个人中，N至少为（ ），就能保证至少两个人生日一样（排除2月29日的情况）的概率大于二分之一。	20	23	150	182
719	判断题	基于Hash的消息认证码的输出长度与消息的长度无关，而与选用的Hash函数有关。	正确	错误		
720	判断题	在相同的硬件平台和软件环境下，相同密钥长度的RSA在加密时硬件实现速度比DES快。	正确	错误		
721	判断题	消息鉴别码中使用的密钥是发送者和接收者之间共享的密钥。	正确	错误		
722	判断题	非线性密码的目的是为了降低线性密码分析的复杂度。	正确	错误		

723	判断题	凯撒密码可以通过暴力破解来破译。	正确	错误		
724	多项选择题	以下属于密码学的分析方法的是（ ）。	差分分析	线性分析	序列分析	结构分析
725	多项选择题	一个密码系统的安全性包含哪些（）。	加密安全性	解密安全性	可证明安全性	计算安全性
726	单项选择题	密码学在信息安全中的应用是多样的，以下不属于密码学的具体应用是（ ）。	网络协议生成	完整性验证	加密保护	身份鉴别
727	单项选择题	密码在信息安全中有广泛的应用，不属于密码具体应用是（ ）。	信息的可用性	信息的完整性	信息的机密性	信息的真实性
728	多项选择题	重合指数密码分析法对以下古典密码算法有效的是（ ）。	置换密码	单表代换密码	多表代换密码	序列密码
729	单项选择题	量子密码与传统的密码系统不同，它主要依赖于（ ）作为安全模式的关键方面。	数学	物理学	化学	电磁
730	单项选择题	2009年是同态加密的里程碑之年, Gentry在他的博士论文中首次提出了（ ）加密的构造框架。	同态	部分同态	全同态	加法同态
731	单项选择题	最佳仿射逼近分析方法是一种（ ）的攻击方法。	选择密文攻击	唯密文攻击	选择明文攻击	已知明文攻击
732	单项选择题	下列攻击方法可用于对消息鉴别码攻击的是（）。	选择密文攻击	字典攻击	查表攻击	密钥推测攻击
733	多项选择题	下列是密码杂凑算法的是（ ）。	MD5	SHA-1	SHA-3	SM3
734	多项选择题	密码设备的各组成部件既可以在多个不同芯片上实现，也可以在单芯片上实现。而模块中常见的属于单芯片构成的密码设备包括以下哪些（ ）。	智能卡	USB Key	密码加速卡	安全芯片
735	多项选择题	对DES的三种主要攻击方法包括（ ）。	暴力攻击	生日攻击	差分密码分析	线性密码分析
736	多项选择题	密码学（cryptology）是研究秘密通信的原理和破译密码的方法的一门科学，密码学包含两个相互独立的分支（ ）。	对称密码	非对称密码	密码编码学	密码分析学

737	多项选择题	密码算法主要分为三类：对称密码算法、非对称密码算法、密码杂凑算法。以下哪两种密码算法属于同一类密码体制（ ）。	RC4和RC5	RSA和DSA	SM4和AES	SM2和SM9
738	多项选择题	公钥密码体制使用不同的加密密钥和解密密钥。以下密码算法是公钥密码体制的有（ ）。	SM2	SM4	Rabin	RSA
739	多项选择题	杂凑函数是一种将任意长度的消息压缩到某一固定长度的消息摘要的函数。以下关于杂凑函数的说法正确的是（ ）。	输入x可以为任意长度；输出数据串长度固定	给定任何x，容易算出H（x）=h；而给出一个杂凑值h，很难找到一特定输入x，使h=H（x）	给出一个消息x，找出另一个消息y使H（x）=H（y）是计算上不可行的	可以找到两个消息x、y，使得H（x）=H（y）
740	多项选择题	消息鉴别是用来验证消息完整性的一种机制或服务。消息鉴别的内容包括（ ）。	证实消息的信源	证实消息内容是否被篡改	保护消息的机密性	保护用户隐私
741	多项选择题	密码杂凑函数是指对不同的输入值，通过密码杂凑函数进行计算，得到固定长度的输出值。对密码杂凑函数的攻击方法有（ ）。	字典攻击	生日攻击	彩虹表攻击	穷举攻击
742	多项选择题	零知识证明包括（ ）两类。	交互式零知识证明	非交互式零知识证明	POW共识机制	POS共识机制
743	多项选择题	一个有新鲜性的值是指这个值是刚产生的，而不是重放的。常用的保证新鲜性的机制有（ ）。	时间戳	一次性随机数	计数器	将时间戳和计数器结合使用的方法
744	多项选择题	根据加、解密时使用密钥的不同，密码体制一般分为（ ）。	对称密码体制	非对称密码体制	分组密码	流密码
745	多项选择题	古典密码的主要方法有（ ）。	代换	加密	隐藏	置换
746	多项选择题	现代密码阶段大约是指20世纪50年代以来的时期。现代密码技术的特点是（ ）。	基于密钥安全	加解密算法公开	加密算法保密	基于置换算法
747	多项选择题	下列密码体制为计算安全的是（ ）。	RSA	ECC	AES	一次一密系统

748	判断题	如果密文中有某一比特始终为常数，则该密文不具备伪随机性。	正确	错误		
749	判断题	如果密文中有某一部分比特始终为常数，则该密文一定不具备不可预测性。	正确	错误		
750	判断题	只使用一个密钥的CBC类MAC，无法保护消息的完整性。	正确	错误		
751	判断题	HMAC是一种消息鉴别码。	正确	错误		
752	多项选择题	以下哪些算法在正确的使用时，同样的密钥对同样的数据执行同样的运算，其结果可能也是不同的。	SM2签名	HMAC-SM3	SM4-ECB	SM2加密
753	判断题	在相同的硬件平台和软件环境下，相同密钥长度的RSA和AES加密速度相同。	正确	错误		
754	判断题	对称密码算法只能C语言实现而不能用其它程序设计语言实现。	正确	错误		
755	判断题	一般来说，常见的加密算法都能用软件实现。	正确	错误		
756	判断题	密码系统的安全性不应取决于不易改变的算法，而应取决于可随时改变的密钥。	正确	错误		
757	判断题	置换密码又叫换位密码，常见的置换密码有栅栏密码等。	正确	错误		
758	单项选择题	字母频率分析法对（ ）算法最有效。	置换密码	单表代换密码	多表代换密码	序列密码
759	单项选择题	GM/Z 4001《密码术语》中，保证信息不被泄露给非授权的个人、进程等实体的性质称为密码的（ ）。	真实性	完整性	机密性	不可否认性
760	单项选择题	GM/T 0006《密码应用标识规范》中的标识符在跨平台传输时，应采用（ ）字节顺序进行传输。	网络字节顺序(Big-endian)	小端(Little-endian)	网络字节序或小端	其它顺序
761	单项选择题	GM/T 0006《密码应用标识规范》定义的标识中，不包括的数据编码格式是（ ）。	DER编码	Huffman编码	Base64编码	PEM编码

762	单项选择题	GM/Z 4001《密码术语》中，一种利用大量互相对应的明文和密文进行分析的密码攻击方法称为（ ）。	线性密码分析	选择明文攻击	选择密文攻击	已知明文攻击
763	判断题	现代密码学中，为了保证安全性，密码算法应该进行保密。	正确	错误		
764	判断题	SM2、SM4、ZUC算法都是对称密码算法。	正确	错误		
765	判断题	衡量一个密码系统的安全性中的无条件安全又称为可证明安全。	正确	错误		
766	判断题	代换密码分为单表代换密码、多表代换密码、转轮密码机。	正确	错误		
767	判断题	GM/T 0006《密码应用标识规范》的用途是对密码算法或数据实体等标识进行统一，以便于密码协议、密码接口间的互联互通。	正确	错误		
768	判断题	GM/T 0006《密码应用标识规范》定义了C和Java等语言实现密码算法时的密钥结构体等具体数据结构。	正确	错误		
769	判断题	Merkle-Hellman密码体制是背包加密体制。	正确	错误		
770	判断题	生日攻击方法利用了Hash函数的结构和代数弱性质。	正确	错误		
771	判断题	抵抗生日攻击方法需要消息摘要必须足够的长。	正确	错误		
772	判断题	时间-存储权衡攻击是一种唯密文攻击。	正确	错误		
773	判断题	NP问题是指用非确定性算法在多项式时间内解决的问题。	正确	错误		
774	判断题	最短向量问题是格上的困难问题。	正确	错误		
775	单项选择题	消息认证（报文鉴别）不能抵抗（ ）攻击。	内容篡改	数据包顺序篡改	伪造消息	侧信道攻击

776	单项选择题	打扑克是一种流行于全世界的休闲类游戏，玩扑克之前首先要进行洗牌，从密码学的角度看，可以将洗牌理解为一种加密运算，目的是让玩家猜不到牌的顺序，那么这种加密运算属于（　）。	置换加密	代换加密	公钥加密	序列加密
777	单项选择题	下列关于未来密码学的发展说法错误的是（　）。	量子计算机能够实现电子计算机所做不到的并行算法	量子计算机能够破解RSA、ECC等密码	进入量子计算时代，仍然需要保护信息的安全，目前使用的密码算法和密钥长度仍然能够保证安全	量子密码的安全性不依赖传统的计算安全
778	多项选择题	根据有限域的描述，下列（ ）是有限域。	模素数n的剩余类集	GF(2的8次方）	整数集	有理数集
779	多项选择题	GB/T 33560-2017《信息安全技术 密码应用标识规范》定义的标识中，包括（ ）。	算法标识	密钥标识	设备标识	协议标识
780	多项选择题	GB/T 33560-2017《信息安全技术 密码应用标识规范》中，包括（ ）的公钥密码算法的标识。	RSA	SM2	ECDSA	SM9
781	多项选择题	GB/T 33560-2017《信息安全技术 密码应用标识规范》》中，包括（ ）的接口标识。	OpenSSL接口	密码设备应用接口	通用密码服务接口	智能IC卡及智能密码钥匙接口
782	多项选择题	GB/T 33560-2017《信息安全技术 密码应用标识规范》中，包括（ ）密钥操作标识。	密钥生成	密钥分发	密钥导入	密钥销毁
783	多项选择题	GB/T 33560-2017《信息安全技术 密码应用标识规范》中，包括（ ）的密钥分类标识。	主密钥	设备密钥	用户密钥	密钥加密密钥
784	多项选择题	下列可以防止重放攻击的方式有（ ）。	时间戳	鉴别方验证序列号没有重复	采用“挑战-响应”机制	数字签名
785	多项选择题	以下关于密钥的描述，正确的是（ ）。	在消息认证码中，发送者和接收者使用共享的密钥来进行认证	在数字签名中，签名的生成和验证使用不同的密钥	消息认证码所使用的密钥，是用于认证的密钥	对称密码和非对称加密的密钥都可以用于机密性保护

786	多项选择题	以下关于完整性保护的说法错误的有（ ）。	在特殊应用中，在确保杂凑值无法被修改时，也可以单纯采用杂凑算法保护数据的完整性	基于公钥密码技术的数字签名可以防止敌手对消息进行篡改，但不能防止接收者对消息进行伪造	基于对称密码或者杂凑算法的完整性保护机制既能确保接收者接收消息之前的消息完整性，也能防止接收者对消息的伪造	HMAC可以避免单独使用杂凑算法可能会遭受中间人攻击的弊端
787	多项选择题	密码学是研究通信安全保密的科学，它包含两个相对独立的分支（ ）。	密码编码学	密码分析学	密钥破译学	密码编译学
788	多项选择题	下列方法可用于对消息认证码攻击的是（ ）。	重放攻击	密钥推测攻击	已知明文攻击	选择密文攻击
789	多项选择题	被周恩来总理称为“龙潭三杰”的地下情报战斗小组，他们是（ ）。	毛泽覃	钱壮飞	李克农	胡底
790	判断题	散列函数的定义中的“任意消息长度”是指实际中存在的任意消息长度，而不是理论上的任意消息长度。	正确	错误		
791	判断题	散列函数的单向性是指根据已知的散列值不能推出相应的消息原文。	正确	错误		
792	多项选择题	以下场景利用了密码的不可否认功能的是（ ）。	网银用户对交易信息进行签名	电子证照	服务端对挑战值进行签名	SSL协议中对会话计算MAC
793	多项选择题	实现和验证不可否认性过程中可能会用到（ ）密码元素。	杂凑函数	时间戳	数字证书验证	签名验签
794	多项选择题	古典密码体制的分析方法有（ ）。	统计分析法	明文-密文分析法	穷举分析法	重合指数法
795	单项选择题	美国数据加密标准DES算法迭代结构是（ ）。	平衡Fesitel网络结构	非平衡Fesitel网络结构	SP结构	MD结构
796	判断题	多表代换密码是以单个代换表对多组明文进行加密。	正确	错误		
797	判断题	古典密码体制的统计分析法是指某种语言中各个字符出现的频率不一样，表现出一定的统计规律。	正确	错误		

798	多项选择题	公开密钥加密（public-key cryptography）也称为非对称密钥加密（asymmetric cryptography），是一种密码学算法类型。下列算法属于公钥密码算法的是（ ）。	RSA算法	ElGamal算法	AES算法	ECC（椭圆曲线密码）算法
799	判断题	多表代换密码是以一系列代换表一次对明文消息的字母序列进行代换的加密方法。	正确	错误		
800	单项选择题	AES密码算法的迭代结构是（ ）。	平衡Fesitel网络结构	非平衡Fesitel网络结构	SP结构	MD结构
801	判断题	古典密码体制重合指数分析法利用随机文本和有意义文本的统计概率差别来分析密码体制。	正确	错误		
802	单项选择题	我国商用密码算法SM4迭代结构是（ ）。	平衡Fesitel网络结构	非平衡Fesitel网络结构	SP结构	MD结构
803	判断题	代换（substitution）密码分为单表代换密码和多表代换密码。	正确	错误		
804	多项选择题	SM4分组密码算法轮函数中的T置换，包括的运算有（ ）。	非线性变换	S盒运算	线性变换	列混合变换
805	单项选择题	在商用密码算法应用中，加密算法（ ）。	可以公开	不能公开 知道	算法只用发送方知道	算法只用接收方
806	多项选择题	在对称分组密码AES中，共进行10轮迭代变换，第10轮进行了的处理变换有（ ）。	字节代换	行移位	列混合	轮密钥加
807	多项选择题	混淆和扩散是密码设计的一般原则，所以在很多密码设计中，都采用了代换和置换等变化来达到混淆和扩散的效果。下列哪些密码体制中，采用了置换的处理思想（ ）。	RSA	CAESAR密码	AES	DES
808	多项选择题	为了提高DES的安全性，并充分利用现有的软硬件资源，人们已设计开发了DES的多种变异版本，下面（ ）属于DES变异版本。	2DES	3DES	4DES	5DES

809	判断题	Nonce是Number once的缩写，在加密技术中的初始向量发挥着重要作用，在各类验证协议的通信应用中确保验证信息不被重复使用以对抗重放攻击。	正确	错误		
810	判断题	分组密码的CTR模式的加密和解密使用了相同的结构，因此易于实现。	正确	错误		
811	判断题	分组密码CTR模式下的消息长度需要是分组长度的整数倍，在加密前需要进行填充操作。	正确	错误		
812	判断题	在PKCS7 Padding的分组密码算法填充方式，每次填充的数量是固定的。	正确	错误		
813	多项选择题	SM4算法的轮函数包括的运算有（ ）。	异或	非线性变换	线性变换	相乘
814	单项选择题	AES算法中，当密钥长度是256位时，分组长度是128位，需要进行加密轮数为（ ）。	6	10	12	14
815	单项选择题	DES算法，有效密钥长度是 ( )位。	44	56	64	128
816	单项选择题	加密算法的工作模式中，ECB指的是（ ）。	密文链接模式	密文反馈模式	输出反馈模式	电码本模式
817	多项选择题	SHANNON于1949年提出了设计对称密码的基本原则，他指出密码设计必须遵循的原则有（ ）。	混淆	扩散	隐藏	拆分
818	单项选择题	SM4加密算法是（ ）。	分组密码体制	序列密码体制	置换密码体制	替代密码体制
819	单项选择题	DES中密钥从输入的64位到输入F函数中，轮密钥长度为（ ）。	64比特	48比特	128比特	36比特
820	单项选择题	IDEA加密算法的的密钥长度为（ ）。	64比特	32 比特	不固定	128比特
821	单项选择题	DES加密算法共经过( )次迭代运算的处理。	8	9	16	18
822	单项选择题	DES加密算法中共用（ ）S盒。	6	7	8	9

823	单项选择题	如果M，C，K分别表示明文、密文和密钥，而M'，C'，K'分别表示的非，E表示加密运算，则DES算法的互补对称性可以表示为（ ）。	C＝E（M，K），则C'＝E（M'，K'）	C＝E（M，K），则C'＝E（M，K）	C＝E（M，K），则C'＝E（M，K'）	C＝E（M，K），则C'＝E（M'，K）
824	多项选择题	AES分组密码算法密钥长度可以是（）。	56比特	128比特	192比特	256比特
825	多项选择题	AES分组密码算法加密过程的轮数可以是（）。	10轮	12轮	14轮	16轮
826	单项选择题	我国商用分组密码算法SM4中使用的S盒的输入是（）位。	4位	6位	8位	16位
827	单项选择题	我国商用分组密码算法SM4中使用的S盒的输出是（）位。	4位	6位	8位	16位
828	单项选择题	分组密码算法AES-192加密的轮数为（）。	10轮	12轮	14轮	16轮
829	单项选择题	分组密码算法AES-128加密的轮数为（）。	10轮	12轮	14轮	16轮
830	单项选择题	分组密码算法AES-256加密的轮数为（）。	10轮	12轮	14轮	16轮
831	单项选择题	我国商用分组密码算法SM4加密的轮数为（）。	12轮	14轮	16轮	32轮
832	单项选择题	AES加密算法中字节代换ByteSub（）是由（ ）运算组合而成。	列混淆	轮密钥加	有限域 GF(2^8)上元素的乘法逆元	对字节仿射变换
833	单项选择题	下面哪种方法不是分组密码体制的分析方法( )。	大整数分解	穷尽密钥搜索	差分密码分析	线性密码分析
834	单项选择题	SM4分组密码算法，该算法的分组长度为128比特，密钥长度为（ ）。	64比特	128比特	192比特	256比特
835	单项选择题	DES算法中扩展运算E的功能是（ ）。	对16位的数据组的各位进行选择和排列，产生一个32位的结果	对32位的数据组的各位进行选择和排列，产生一个48位的结果	对48位的数据组的各位进行选择和排列，产生一个64位的结果	对56位的数据组的各位进行选择和排列，产生一个64位的结果
836	单项选择题	Skipjack是一个密钥长度为（ ）位分组加密算法。	56	64	80	128

837	单项选择题	一个消息明文长度为740比特，使用SM4算法进行加密时，以下哪种模式不需要对该明文填充至6个分组长度。	CBC	CTR	CFB	ECB
838	单项选择题	SM4算法的密钥和明文长度分别是多少比特（ ）。	128、256	128、128	256、128	256、256
839	多项选择题	AES由四个不同的模块组成，其中不是非线性模块的有（ ）。	字节代换	行位移	列混淆	轮密钥加
840	多项选择题	Shannon建议密码设计的基本方法包括（ ）。	布尔运算	扩散	混淆	迭代
841	多项选择题	分组密码算法有（ ）工作模式。	ECB	CBC	CFB	OFB
842	多项选择题	为保证安全性，在设计分组密码时应该考虑（ ）等问题。	在设计分组密码时，加密/解密变换必须足够复杂	加密时间要足够长	密钥空间足够大	解密时间要足够长
843	多项选择题	下列（ ）不属于分组密码体制。	ECC	IDEA	RC5	ElGamal
844	多项选择题	AES算法的步骤有（ ）。	字节代替	行移位	列混淆	轮密钥加
845	多项选择题	为保证安全性，在设计分组密码时，密码变换必须足够复杂，尽量使用（ ）原则。	混淆	可重复性	保密性	扩散
846	判断题	密码术语上，计数器值一定是随机数。	正确	错误		
847	判断题	CTR加密模式具备并行计算的特点。	正确	错误		
848	判断题	SM4算法中解密轮密钥是加密轮密钥的逆序。	正确	错误		
849	判断题	3DES也称为TDEA，该算法是将明文进行三次DES运算，其中包含一次DES解密计算。	正确	错误		
850	单项选择题	如果 DES 加密使用的轮密钥为k1,k2……k16，则 DES 解密时第一轮使用的密钥为( )。	k1	k8	k12	k16
851	单项选择题	在IDEA中，有( )个加密轮次。	16	12	8	10

852	单项选择题	AES 算法中的状态可表示为一个二维数组，如果明文长度为 128 比特，则明文状态为（ ）。	4行4列	4行6列	4行8列	4行10列
853	单项选择题	下面关于 AES 算法的叙述，哪一个是正确的（ ）。	AES 算法是用 56 比特的密钥加密 64 比特的明文得到 64 比特的密文	AES 算法属于非对称密码算法	AES 是一个数据块长度和密钥长度可分别为 128 比特、192 比特或 256比特的分组密码算法	AES 是一个数据块长度和密钥长度可分别为 64 比特或 128 比特的分组密码算法
854	单项选择题	在下面分组密码加密工作模式中，有密文传输错误扩散的是（ ）。	ECB	OFB	CBC	CTR
855	多项选择题	DES的三种主要的攻击方法是（ ）。	穷举攻击	差分密码分析	线性密码分析	查表攻击
856	判断题	类似于AES算法的S盒，SM4算法的S盒也是基于有限域逆运算构造。	正确	错误		
857	判断题	SM4算法采用的8比特S盒与AES算法的S盒满足仿射等价关系。	正确	错误		
858	判断题	SM4在整体结构上采用的是Source-Heavy型广义Feistel结构。	正确	错误		
859	判断题	SM4在整体结构上采用的是Target-Heavy型广义Feistel结构。	正确	错误		
860	判断题	在SM4密钥扩展算法中，首先需要将主密钥与128位系统参数异或。	正确	错误		
861	判断题	SM4加密算法的轮密钥由加密密钥通过密钥扩展算法生成。	正确	错误		
862	判断题	SM4解密算法的轮密钥也由主密钥通过密钥扩展算法生成，只是按逆序使用。	正确	错误		
863	判断题	SM4算法采用的8比特S盒与AES算法的S盒满足线性等价关系。	正确	错误		
864	判断题	SM4算法采用32轮非线性迭代结构，以32比特字为单位进行加密运算，一次迭代为一轮变换。	正确	错误		
865	判断题	对于SM4算法的S盒，每一个非零的输入差分，对应127个可能的输出差分。	正确	错误		

866	判断题	SM4算法中，其反序变换与算法的安全强度相关。	正确	错误		
867	判断题	SM4分组密码的解密算法与加密算法结构相同，只是解密轮密钥是加密轮密钥的逆序。	正确	错误		
868	判断题	SM4算法的S盒为固定的8比特输入8比特输出的置换。	正确	错误		
869	判断题	SM4加密算法采用 32 轮非线性迭代结构。	正确	错误		
870	判断题	SM4密钥扩展算法采用 32 轮非线性迭代结构。	正确	错误		
871	判断题	SM4加密算法与密钥扩展算法中的轮函数完全相同。	正确	错误		
872	判断题	SM4加密算法与密钥扩展算法中的轮函数基本相同，只将线性变换进行了修改。	正确	错误		
873	判断题	为了抵抗滑动攻击等，密钥扩展算法通常需要使用轮常数，SM4中的轮常数为轮数的二进制表示。	正确	错误		
874	判断题	SM4加密算法的轮函数是可逆的。	正确	错误		
875	判断题	不同于DES算法，SM4算法的密钥是128位，其中密钥有效位也是128位。	正确	错误		
876	判断题	SM4算法的分组长度是128位。	正确	错误		
877	判断题	类似于AES算法，SM4算法的密钥长度也可以是128、192、256位。	正确	错误		
878	判断题	SM4加密算法中，除32轮迭代外，最后还需要经过一个反序变换。	正确	错误		
879	判断题	类似于加密算法，SM4密钥扩展算法的最后也需要经过一个反序变换。	正确	错误		
880	判断题	SM4密钥扩展算法采用了32个固定参数作为轮常数。	正确	错误		
881	判断题	SM4算法是一个分组长度和密钥长度均为128位的分组加密算法。	正确	错误		

882	判断题	我国自主研制的SM4分组密码算法广泛应用于数据保密传输、信息加密存储等应用领域。	正确	错误		
883	判断题	SM4算法的分组长度和密钥长度可以不一样。	正确	错误		
884	判断题	SM4算法的线性变换L不存在固定点。	正确	错误		
885	判断题	SM4算法的线性变换L不可逆。	正确	错误		
886	单项选择题	IDEA的分组长度是（ ）比特。	56	64	96	128
887	单项选择题	对称密码算法ECB模式指的是（ ）。	密文链接模式	密文反馈模式	输出反馈模式	电码本模式
888	单项选择题	对称密码算法CFB模式指的是（ ）。	计数器模式	密文反馈模式	输出反馈模式	密文链接模式
889	多项选择题	以下分组密码算法工作模式不需要填充的是（ ）。	CTR	CFB	CBC	OFB
890	多项选择题	磁盘加密要求密文和初始向量等的总长度不会超过原有的明文长度，以下分组工作模式适合用于磁盘加密的是（ ）。	XTS	HCTR	CTR	ECB
891	多项选择题	以下操作方式，可能出现安全问题的是（ ）。	使用ECB对于RGB图片进行加密	使用固定IV的CBC模式进行性别的加密	明文传递CTR模式的计数器值	未采用可靠方式传递根CA的自签名证书
892	多项选择题	以下（ ）算法可以安全地为变长的数据生成MAC。	CBC-MAC	HMAC	GCM	CMAC
893	多项选择题	关于分组密码算法工作模式描述正确的是（ ）。	ECB和CTR模式的加密和解密过程均支持并行计算	CFB、OFB和CTR模式在加密时不需要填充操作	在ECB模式下，若某些密文分组比特错误，则解密后对应的明文分组也会出错	在CBC模式解密中，如果密文分组1损坏，但是密文2、3没有损坏，则密文分组3是无法正确解密的

894	多项选择题	以下分组密码算法工作模式，说法是正确的（ ）。	在CRT模式中，主动攻击者可以通过反转密文分组中的某些比特，引起解密后明文中的相应比特也发生反转。	在OFB模式中，可以在加密消息之前预计算密钥流	CFB模式与OFB模式的区别仅仅在于密码算法的输入。	假设CBC模式加密的密文分组中有一个分组损坏了（如由于硬盘故障导致密文分组的值发生了改变），在这种情况下，只要密文分组的长度没有发生变化，则解密时最多只会有2个分组受到数据损坏的影响。
895	多项选择题	以下分组密码算法的工作模式IV要求每个消息必须唯一，不能重用，且不可预测的是（ ）。	OFB	CFB	CBC	GCM
896	判断题	CCM不仅能加密数据，还能够保护数据的完整性。（ ）	正确	错误		
897	判断题	OCB可鉴别加密模式不能够保护数据的完整性。（ ）	正确	错误		
898	判断题	OFB能够保护数据的真实性。（ ）	正确	错误		
899	单项选择题	在AES算法中每一轮的轮密钥的长度为（ ）位。	64	128	256	512
900	单项选择题	DES加密算法对输入的明文首先进行（ ）。	左右分离	初始置换	迭代运算	乘法运算
901	单项选择题	在2012年，国家密码管理局发布了一系列国产密码算法作为密码行业标准，其中（ ）是分组密码。	祖冲之算法	SM4算法	SM2算法	SM3算法
902	单项选择题	广泛应用于商用数据保密的我国自主研制的分组密码算法是（ ）。	3DES	IDEA	AES	SM4
903	单项选择题	以下4个不同的变换，其中（ ）不是SM4算法轮函数的组成模块。	S盒变换	行位移	线性变换L	轮密钥异或
904	单项选择题	当SM4算法采用（ ）工作模式时，可以并行处理多组消息分组。	ECB	CBC	CFB	OFB

905	单项选择题	下述（ ）密码算法是分组密码算法。	SM2	SM3	SM4	SM9
906	单项选择题	SM4算法的轮密钥由加密密钥生成，共有（ ）个轮密钥。	4	31	32	128
907	单项选择题	SM4是我国提出的商用密码算法，SM4算法进行密钥扩展时的迭代次数是（ ）。	8	16	31	32
908	单项选择题	SM4是我国提出的商用密码算法，SM4算法进行加解密时的迭代次数是（ ）。	10	16	31	32
909	单项选择题	SM4算法的轮密钥由加密密钥生成，每个轮密钥为（ ）比特字。	8	32	64	128
910	单项选择题	SM4密钥扩展算法中首先将加密密钥与（ ）异或。	系统参数	固定参数	轮常数	明文
911	单项选择题	SM4算法的非线性变换由（ ）个并行的S盒构成。	4	8	16	32
912	单项选择题	SM4加密轮函数中的线性变换L的输入为（ ）比特。	8	32	128	160
913	多项选择题	分组密码将明文消息编码表示后的数字序列进行分组划分并进行加密，下列不属于分组密码体制的有（ ）。	SM2密码体制	IDEA密码体制	RC5密码体制	ElGamal密码体制
914	多项选择题	下列关于分组密码算法的设计的说法正确的是（ ）。	分组长度应足够大，以防止明文被穷举攻击	密钥空间应足够大，尽可能消除弱密钥	密钥越长，安全性越强，因此，设计的密钥长度应该很长	由密钥确定的算法要足够复杂，要能抵抗各种已知的攻击
915	多项选择题	对称密码的优点是非常快速，受到广泛的应用，选项中哪些是对称密码算法（ ）。	RSA算法	3DES算法	SM4算法	IDEA算法
916	多项选择题	以下属于分组密码算法的是（ ）。	RC4	SM4	RSA	IDEA
917	多项选择题	下列属于分组密码的主要模式是（ ）。	ECB	CBC	CFB	OFB
918	判断题	分组密码工作模式的安全性与底层分组密码的分组长度无关。	正确	错误		
919	判断题	不具备可证明安全理论保障的分组密码工作模式一定不安全。	正确	错误		

920	判断题	具备可证明安全理论保障的分组密码工作模式可在现实中抵抗所有攻击方式。	正确	错误		
921	判断题	MAC算法确保消息的MAC由只有通信双方知道的秘密密钥K来控制，将MAC算法的输出截断后再发送，不降低实用安全强度。	正确	错误		
922	判断题	消息鉴别码生成的标签必须随同消息一起加密发送给对方。	正确	错误		
923	判断题	分组密码的可鉴别的加密模式可同时保护数据的机密性和完整性。	正确	错误		
924	判断题	CTR加密模式在解密过程中需要执行分组密码的解密操作。	正确	错误		
925	判断题	CBC加密模式在解密过程中需要执行分组密码的解密操作。	正确	错误		
926	判断题	OFB加密模式在解密过程中需要执行分组密码的解密操作。	正确	错误		
927	判断题	CFB加密模式在解密过程中需要执行分组密码的解密操作。	正确	错误		
928	判断题	CTR加密模式是分组密码的一种常见的工作模式，该模式下不具备错误扩散性。	正确	错误		
929	判断题	使用各自独立密钥的分组密码加密模式和MAC模式，可以构造一个认证加密模式。	正确	错误		
930	判断题	分组密码工作模式在使用前，需要消息（或密文）收发双方共享对称密钥。	正确	错误		
931	判断题	分组密码的分组长度是衡量分组密码工作模式设计质量的参数之一。	正确	错误		
932	判断题	分组密码认证模式的构造可以抽象为使用PRP构造PRF。	正确	错误		
933	判断题	分组密码的确定性可鉴别加密模式仍然需要随机IV或Nonce保障安全性。	正确	错误		
934	判断题	分组密码的确定性可鉴别加密模式模式可通过MAC-then-Enc的方式构造。	正确	错误		

935	判断题	在收到消息和MAC后，收方使用同一密钥产生MAC值，通过对比新产生的MAC和收到的MAC是否相同，确认消息是否合法。	正确	错误		
936	判断题	在收到分组密码CBC产生的密文后，收方即便使用密钥也无法百分百确认密文的完整性。	正确	错误		
937	判断题	保序加密使得有顺序的明文加密之后依然保持顺序，分组密码的保序加密总是使得密文和明文相同长度。	正确	错误		
938	判断题	CBC（Cipher-Block-Chaining）是经典的密码工作模式，每个明文块先与前一个密文块进行异或后，再进行加密，是一类典型的并行结构。	正确	错误		
939	判断题	黑盒模型下具备生日界的CBC-MAC，在量子攻击下不再安全。	正确	错误		
940	单项选择题	为确保加解密结构一致，SM4算法最后还需经过一次（ ）运算。	反序变换	交叉变换	非线性变换	正形置换
941	单项选择题	SM4加密轮函数中的线性变换由输入及其循环左移若干比特共（ ）项异或而成。	4	5	8	32
942	单项选择题	SM4密钥扩展算法中的线性变换由输入及其循环左移若干比特共（ ）项异或而成。	3	4	5	32
943	单项选择题	下述哪些变换（ ）与SM4算法的安全强度无关。	S盒变换	线性变换	轮密钥异或加变换	反序变换
944	单项选择题	下列关于SM4分组密码算法叙述错误的是（ ）。	一般来说，分组密码迭代轮数越多，密码分析越困难	可以用于数据加密	是对称密码	是不可逆的
945	单项选择题	下述关于SM4算法和AES算法采用的S盒之间的关系叙述错误的是（ ）。	都是8比特输入8比特输出的非线性置换	都是基于有限域逆运算构造	两者之间线性等价	两者之间仿射等价
946	单项选择题	下述（ ）运算是SM4算法中线性变换L的基本运算。	循环左移	循环右移	左移	右移

947	单项选择题	下列关于SM4分组密码算法叙述正确的是（ ）。	一次只对明文消息的单个字符进行加解密变换	是不可逆的	采用了正形置换设计思想	需要密钥同步
948	单项选择题	下列关于SM4的解密算法叙述错误的是（ ）。	解密算法与加密算法结构相同	解密轮密钥与加密轮密钥相同	解密轮密钥是加密轮密钥的逆序	解密算法与加密算法都采用32轮迭代
949	单项选择题	下列关于SM4的密钥扩展算法叙述错误的是（ ）。	采用32轮非线性迭代结构	每次迭代生成32比特轮密钥	采用与加密算法相同的S盒	采用与加密算法相同的线性变换
950	单项选择题	SM4加密算法的线性变换L存在（ ）个固定点。	0	1	2	4
951	单项选择题	下列分组密码加密模式，加密过程中可并行生成伪随机流的是（ ）。	CBC	OFB	CFB	CTR
952	单项选择题	下列基于分组密码的MAC模式，使用并行结构的是（ ）。	OMAC	TMAC	EMAC	PMAC
953	单项选择题	下列分组密码工作模式，（ ）是可鉴别的加密模式。	CBC-MAC	PMAC	EtM	ECB
954	单项选择题	消息鉴别码比杂凑函数增加了（ ）功能。	机密性保护	完整性保护	消息源鉴别	不可否认性
955	单项选择题	标准的Enc-then-MAC需要使用（ ）个独立随机密钥。	一个	两个	三个	四个
956	单项选择题	消息鉴别码需要具备的最低安全性是（ ）。	PRF	不可预测	PRP	SPRP
957	单项选择题	底层采用SM4算法的生日界安全分组密码工作模式，抵抗区分攻击的强度接近于（ ）。	2^32	2^64	2^128	2^256
958	单项选择题	下列分组密码加密模式，解密过程中具备错误扩散的是（ ）。	CBC	OFB	CFB	CTR
959	单项选择题	分组密码工作模式在使用过程中，（ ）等参数必须严格保密。	Nonce	计数器	密钥	随机IV
960	多项选择题	在SM4算法的线性变换中，循环左移运算的移位数包括（ ）。	2	10	18	24
961	多项选择题	对于SM4分组密码，当采用CTR工作模式时，下述描述正确的是（ ）。	具有良好的硬件和软件效率	能进行随机访问	可以在明文到来之前计算密钥流	不能用于高速实现需求

962	多项选择题	SM4算法中采用了下述（ ）基本运算。	异或运算	模幂运算	移位运算	循环移位运算
963	多项选择题	SM4算法轮函数中的合成置换T由下述选项中哪几个（ ）复合而成。	扩展置换	初始置换	非线性变换	线性变换
964	多项选择题	SM4分组密码主要采用（ ）原则来抵抗攻击者的统计分析。	混淆	自逆	对称	扩散
965	多项选择题	下列关于SM4算法的描述中，正确的是（ ）。	SM4算法的加密过程由连续的32轮迭代和一个反序变换组成	SM4算法的每轮迭代中更新32比特数据	SM4算法的32轮迭代中，每一轮都需要1个32比特的轮密钥	SM4算法的明文、密文和密钥的长度都为128比特
966	多项选择题	SM4算法在电子密码本(ECB，Electronic Code Book)模式下容易受到下述哪些攻击（ ）。	统计分析攻击	分组重放攻击	代换攻击	差分攻击
967	多项选择题	下述（ ）算法的S盒与SM4算法的S盒是仿射等价。	DES	AES	Camellia	MISTY
968	多项选择题	SM4分组密码算法可以用于下列哪些用途（ ）。	数据保密传输	信息加密存储	签名认证	消息鉴别码
969	多项选择题	下述正确描述SM4和AES有什么不同之处的是（ ）。	SM4密钥长度固定，而AES密钥长度可变	SM4的线性变换是面向比特的运算，而AES的所有运算是面向字节的	SM4的加密过程和解密过程一致，而AES的加密过程和解密过程不一致	SM4是非平衡广义Fesitel结构，而AES是SP结构
970	多项选择题	SM4算法由国家密码管理局发布，下列是正确描述SM4算法是（ ）。	SM4是一种分组密码算法	SM4分组长度为128比特	SM4密钥长度为128比特	SM4加密算法的迭代次数为32
971	多项选择题	在SM4密钥扩展算法的线性变换中，循环左移运算的移位数包括（ ）。	8	13	23	24
972	多项选择题	下述正确描述SM4的是（ ）。	SM4目前ISO/IEC标准化组织采纳	SM4的分组长度为128位	SM4的密钥长度为128位	SM4原名SMS4
973	多项选择题	评估SM4算法的安全性，必须考虑下述对分组密码算法常用的分析方法（ ）。	差分分析	线性分析	不可能差分分析	积分分析

974	多项选择题	下述对SM4分组密码算法介绍中正确的是（ ）。	将消息分为固定长度的数据块来逐块处理的	分组长度和密钥长度一样长	分组长度和密钥长度不一样	加密算法中的线性变换与密钥扩展算法中的线性变换完全一致
975	多项选择题	当SM4算法采用（ ）工作模式时，可以采用流水线技术优化实现。	ECB	CBC	CFB	CTR
976	多项选择题	下列分组密码工作模式中，解密过程支持并行计算的有（ ）。	CBC	CTR	ECB	XTR
977	多项选择题	下列分组密码工作模式中，解密之前可以进行伪随机流预计算的有（ ）。	CBC	CTR	OFB	CFB
978	多项选择题	分组密码的可鉴别的加密模式，可以保护数据的（ ）。	机密性	不可否认性	完整性	数据起源认证
979	多项选择题	分组密码的认证加密模式与公钥体制下的数字签名相比，（ ）不是共有的。	保护数据机密性	保护数据完整性	不可否认性	运行速度快
980	多项选择题	分组密码的认证模式与公钥体制下的数字签名相比，（ ）是共有的。	保护数据机密性	保护数据完整性	数据起源认证	运行速度快
981	多项选择题	下列分组密码工作模式中，加密过程只能串行计算的有（ ）。	CBC	CTR	OFB	CFB
982	多项选择题	下列分组密码工作模式，属于认证加密模式的有（ ）。	OMAC	CCM	EAX	ECB
983	多项选择题	底层采用SM4算法的EMAC，输出标签的比特长度支持（ ）。	32	64	128	256
984	多项选择题	不借助其他密码机制，分组密码算法自身可实现（ ）。	加密功能	认证功能	数据摘要功能	数字签名功能
985	多项选择题	下列分组密码工作模式，解密过程中不需要调用分组密码解密算法的是（ ）。	CBC	OFB	CFB	CTR
986	多项选择题	下列分组密码可鉴别的加密模式，解密过程中一定不需要调用分组密码解密算法的是（ ）。	GCM	OCB	CCM	EAX
987	多项选择题	为保障分组密码工作模式的实用安全性，通常采用的措施有（ ）。	控制明文长度上限	经常更新加密密钥	多次加密同一明文	规范使用Nonce、IV等参数

988	多项选择题	下列分组密码可鉴别的加密模式，使用串行结构的包括（ ）。	OMAC	XCBC	PMAC	EMAC
989	多项选择题	下列分组密码工作模式中，加密不能并行但解密可并行的是（ ）。	CBC	OFB	CFB	CTR
990	多项选择题	下列分组密码工作模式中，在解密过程中不需要调用分组密码逆运算的有（ ）。	CBC	CTR	OFB	CFB
991	多项选择题	下列分组密码加密模式中，加密过程具备错误扩散的有（ ）。	CBC	ECB	CTR	CFB
992	多项选择题	分组密码的认证加密模式在应用过程中，可以输出的信息有（ ）。	Nonce	密文	标签	密钥
993	多项选择题	分组密码认证模式的特点包括（ ）。	机密性保护	完整性保护	数据起源认证	速度快
994	多项选择题	以下密码结构，具备逆变换的有（ ）。	Feistel	MISTY	Sponge	Benes
995	判断题	DES算法可以用软件实现，也可以用硬件实现。	正确	错误		
996	判断题	差分密码分析利用的是密码体制的高概率差分。	正确	错误		
997	判断题	线性密码分析方法本质上是一种已知明文攻击的攻击方法。	正确	错误		
998	判断题	非线性密码分析的目的是为了降低线性密码分析的复杂度。	正确	错误		
999	单项选择题	下列分组密码认证加密模式中，（ ）只需对明文处理一遍。	Enc-then-MAC	OCB	GCM	CCM
1000	单项选择题	下列分组密码工作模式，未采用并行结构的是（ ）。	CMAC	OCB	PMAC	CTR
1001	单项选择题	下列分组密码认证模式中，使用密钥最少的是（ ）。	OMAC	TMAC	XCBC	EMAC
1002	单项选择题	底层采用SM4算法的生日界安全分组密码工作模式，抵抗密钥恢复攻击的强度接近于（ ）。	2^32	2^64	2^128	2^256
1003	单项选择题	采用SM4算法的CBC-MAC，其输出的标签无法支持（ ）比特长度。	32	64	128	256
1004	单项选择题	CTR是一种分组密码（ ）模式。	加密	认证	认证加密	杂凑
1005	单项选择题	OFB是一种分组密码（ ）模式。	加密	认证	认证加密	杂凑
1006	单项选择题	Enc-then-MAC是一种（ ）模式。	加密	认证	认证加密	杂凑

1007	单项选择题	下列分组密码工作模式，能够保护数据完整性的是（ ）。	CTR	OFB	CBC-MAC	ECB
1008	单项选择题	下列分组密码工作模式，能够保护数据机密性的是（ ）。	EMAC	CMAC	PMAC	CTR
1009	单项选择题	下列不属于对称密码体制的是（ ）。	分组密码认证模式	分组密码加密模式	分组密码认证加密模式	数字签名
1010	单项选择题	在量子攻击下，根据Grover算法，采用SM4的分组密码CTR模式抵抗密钥恢复攻击的强度大约是（ ）。	2^32	2^64	2^96	2^128
1011	单项选择题	如果泄漏了CBC-MAC的链接值，会导致如下情况发生（ ）。	密钥被恢复	CBC-MAC被伪造（消息、标签）	生成标签错误	无任何问题
1012	多项选择题	下列分组密码工作模式，能够保护数据机密性的是（ ）。	CTR	OMAC	GCM	OFB
1013	多项选择题	下列分组密码工作模式，能够保护数据完整性的是（ ）。	CTR	OMAC	GCM	OFB
1014	单项选择题	关于DES加密算法和AES加密算法的说法中错误的是（ ）。	DES是一个分组算法，数据分组长度为64比特位	AES是一个分组密码算法，数据分组长度为128比特位	DES和AES均为对称密钥加密算法	DES和AES密钥长度为128比特位（16字节）
1015	单项选择题	SM4的解密和加密使用相同的算法，只是将（ ）的使用次序反过来。	明文	密文	轮密钥	密钥
1016	单项选择题	DES算法密钥是64位，其中密钥有效位为（ ）。	32比特	56比特	64比特	128比特
1017	单项选择题	下述（ ）密码算法是分组密码算法。	SHA-1	A5	IDEA	RSA
1018	单项选择题	AES在整体结构上采用的是（ ）结构。	Square	Feistel	Sponge	SP
1019	单项选择题	下列分组密码工作模式中，加解密均支持并行计算的是（ ）。	CBC	OFB	CFB	CTR
1020	单项选择题	GCM是一种分组密码（ ）模式。	加密	认证	认证加密	杂凑

1021	单项选择题	某业务员发起了“从A账户向B账户转账1亿元”的转账请求数据并进行加密传输，攻击者将捕获的密文分组数据进行对调，将原转账请求内容改为了“从B账户向A账户转账1亿元”，以下加密模式可能会导致该问题发生的是（ ）。	CBC	ECB	BC	CFB
1022	单项选择题	CCM是CTR工作模式和CBC-MAC消息鉴别码以（ ）的形式进行结合。	MAC-then-Encrypt	Encrypt-then-MAC	Encrypt-and-MAC	Hash-then-Encrypt
1023	多项选择题	分组密码的短块加密方法主要有（ ）。	填充法	序列密码加密法	输出反馈模式	密文挪用技术
1024	多项选择题	DES 算法的主要缺点有（ ）。	密钥比较短	存在弱密钥	算法为对称运算	存在互补对称性
1025	多项选择题	以下（ ）是DES的工作模式。	ECB	CBC	非对称反馈模式	OFB
1026	多项选择题	以下哪种算法属于分组密算法的是（ ）。	IDEA	RC4	Blowfish	RC5
1027	多项选择题	以下关于分组密码正确说法的是（ ）。	分组密码的结构一般可以分为两种：Feistel网络结构和SP网络结构	DES算法是Feistel结构的一个代表，AES算法、SM4算法是SP结构的代表	分组密码由加密算法、解密算法和密钥扩展算法三部分组成	Feistel网络解密过程与其加密过程实质是相同的，而SP网络密码可以更快的得到扩散，但加、解密过程通常不相似
1028	多项选择题	以下分组密码的工作模式类似于流密码的是（ ）。	CFB	CBC	CTR	OFB
1029	判断题	CTR加密模式在使用中必须保证计数器的唯一性。	正确	错误		
1030	判断题	计数器可以被认为是一种Nonce生成方法。	正确	错误		
1031	判断题	简单地说，分组密码的SP结构就是顺序地执行两个或多个基本密码系统，使最后结果的密码强度高于每个密码系统的结果。	正确	错误		

1032	判断题	AES分组密码算法采用的总体结构类型为Feistel结构。	正确	错误		
1033	判断题	三重DES算法的有效密钥长度为192位。	正确	错误		
1034	判断题	对称密码体制的特征是加密密钥和解密密钥完全相同。	正确	错误		
1035	单项选择题	序列密码的安全性主要基于（ ）。	加密算法	密钥序列生成算法	解密算法	鉴别方法
1036	单项选择题	初始状态为(00...0)的线性反馈移位寄存器输出序列的周期是( )。	不能确定	1	0	无穷大
1037	单项选择题	初始状态为(11…1)的线性反馈移位寄存器输出序列的周期是( )。	不能确定	1	0	无穷大
1038	单项选择题	ZUC-128算法是一个面向字的序列密码，密钥长度为（ ）。	64比特	128比特	256比特	1024比特
1039	单项选择题	ZUC-128算法是一个面向字的序列密码，初始向量的长度为（ ）。	64比特	128比特	256比特	1024比特
1040	单项选择题	ZUC-128主算法一次输出的密钥流长度为（ ）。	32比特	64比特	128比特	256比特
1041	单项选择题	SM3密码杂凑函数的迭代结构是（ ）。	Feistle迭代结构	SP结构	MD结构	Sponge结构
1042	单项选择题	SHA-3密码杂凑函数的结构是（ ）。	Feistel结构	SP结构	MD结构	Sponge结构
1043	多项选择题	线性移位反馈寄存器输出序列的周期与（ ）有关。	初始状态	初始状态唯一决定	结构常数	反馈函数
1044	判断题	ZUC算法是一个序列密码算法。	正确	错误		
1045	判断题	ZUC算法是中国自主设计的密码算法。	正确	错误		
1046	判断题	ZUC算法是一个基于字设计的序列密码算法。	正确	错误		
1047	判断题	ZUC算法是一个自同步序列密码算法。	正确	错误		
1048	判断题	ZUC算法的全称为祖冲之算法。	正确	错误		
1049	判断题	ZUC算法LFSR部分可以产生素域上的m序列作为算法的源序列。	正确	错误		
1050	判断题	ZUC算法的非线性函数F的设计借鉴了分组密码的设计思想。	正确	错误		

1051	判断题	ZUC算法LFSR部分移位寄存器每个单元为32比特的字。	正确	错误		
1052	判断题	ZUC算法初始化过程中非线性函数F的输出直接参与到LFSR的反馈运算中。	正确	错误		
1053	判断题	ZUC算法非线性函数F部分两个线性变换L1和L2的矩阵均为MDS矩阵。	正确	错误		
1054	判断题	ZUC算法非线性函数F部分仅使用3个S-盒。	正确	错误		
1055	判断题	ZUC算法非线性函数F部分使用的S-盒其中之一基于有限域逆函数构造，与AES算法的S-盒类似。	正确	错误		
1056	判断题	ZUC算法是一个分组密码算法。	正确	错误		
1057	判断题	ZUC算法2016年被发布为国家标准。	正确	错误		
1058	判断题	ZUC算法LFSR部分使用环上LFSR，因而实现代价较高。	正确	错误		
1059	判断题	ZUC算法比特重组层BR抽取的4个32比特字全部参与于非线性函数F的运算。	正确	错误		
1060	判断题	ZUC算法是一个同步序列密码算法。	正确	错误		
1061	判断题	ZUC算法密钥产生阶段非线性函数F的运算结果直接作为密钥流输出。	正确	错误		
1062	判断题	以ZUC算法为核心的128EIA-3算法为MAC算法。	正确	错误		
1063	判断题	ZUC算法非线性函数F部分使用的S-盒均具有较低代数免疫度，严重影响算法的安全性。	正确	错误		
1064	判断题	ZUC算法非线性函数F部分两个线性变换L1和L2的设计使用了右循环移位运算。	正确	错误		
1065	判断题	ZUC算法密钥流产生阶段每一拍产生31比特长的密钥流。	正确	错误		
1066	判断题	ZUC算法存在碰撞型弱密钥。	正确	错误		
1067	判断题	ZUC算法在整体结构上与Grain128算法类似。	正确	错误		

1068	判断题	ZUC算法在整体结构上与SNOW3G算法类似。	正确	错误		
1069	判断题	ZUC算法非线性函数F部分两个记忆单元的长度均为31比特。	正确	错误		
1070	判断题	ZUC算法密钥载入时需要使用16个15比特长的常数。	正确	错误		
1071	判断题	ZUC算法LFSR部分产生的二元序列具有很低的线性复杂度。	正确	错误		
1072	判断题	ZUC算法LFSR部分产生的二元序列具有较大周期。	正确	错误		
1073	多项选择题	以下属于序列密码算法的是（ ）。	ZUC	RC5	RC6	RC4
1074	判断题	ZUC算法是中国国家密码管理局发布的一种流密码算法，是中国的国家密码标准之一。ZUC算法的驱动部分采用了带进位的线性反馈移位寄存器。	正确	错误		
1075	判断题	ZUC算法初始化轮数为32。	正确	错误		
1076	判断题	ZUC算法密钥载入时两个记忆单元的值均设置为0。	正确	错误		
1077	判断题	ZUC算法比特重组BR层主要使用了右移位操作。	正确	错误		
1078	判断题	ZUC-128算法的密钥长度为128比特，IV值长度也为128比特。	正确	错误		
1079	单项选择题	以ZUC算法为核心算法的保密性和完整性算法在（ ）年成为3GPP LTE标准。	2009	2010	2011	2012
1080	单项选择题	ZUC算法是一个（ ）密码算法。	分组	序列	公钥	杂凑
1081	单项选择题	ZUC算法的LFSR部分采用（ ）产生算法的源序列。	线性移位寄存器	带进位反馈移位寄存器	非线性反馈移位寄存器	T-函数
1082	单项选择题	ZUC算法的LFSR部分中移位寄存器总长度为（ ）比特。	480	496	512	528
1083	单项选择题	ZUC算法比特重组部分从寄存器单元抽取（ ）比特供非线性函数和密钥导出函数使用。	64	128	192	256
1084	单项选择题	ZUC算法密钥流产生阶段每一拍产生（ ）比特长的密钥流。	1	8	16	32

1085	单项选择题	ZUC算法LFSR部分产生二元源序列的周期约为（ ）。	2^{128}	2^{256}	2^{496}	2^{512}
1086	单项选择题	ZUC算法LFSR部分由16个（ ）比特的字单元变量构成。	8	16	32	31
1087	单项选择题	ZUC算法的非线性函数F没有采用（ ）运算。	模2^{31}-1的加法	模2^{32}的加法	比特级异或	左循环移位
1088	单项选择题	ZUC算法的非线性函数F的设计采用了4个（ ）比特的S盒。	4×4	8×8	16×16	32×32
1089	单项选择题	ZUC算法非线性函数F部分包含2个（ ）比特的记忆单元。	8	16	32	64
1090	单项选择题	ZUC算法驱动部分的设计使用了模（ ）的环上的LFSR。	2^{31}	2^{31}-1	2^{32}	2^{32}-1
1091	单项选择题	ZUC算法密钥载入时两个记忆单元的值设置为（ ）。	全1比特串	全0比特串	随机比特串	种子密钥
1092	单项选择题	ZUC算法初始化轮数为（ ）。	65	64	35	32
1093	单项选择题	ZUC算法初始化过程中非线性函数F的输出需要（ ）参与到LFSR的反馈运算中。	左移一位	右移一位	循环左移一位	循环右移一位
1094	单项选择题	ZUC算法在（ ）年被发布为国家标准。	2009	2011	2012	2016
1095	单项选择题	ZUC算法非线性函数F部分共使用（ ）个8比特S-盒。	2	4	6	8
1096	单项选择题	以ZUC算法为核心的128EEA-3算法为（ ）。	保密性算法	公钥算法	完整性算法	签名算法
1097	单项选择题	以ZUC算法为核心的128EIA-3算法为（ ）。	保密性算法	公钥算法	完整性算法	签名算法
1098	单项选择题	ZUC算法在（ ）年被发布为国家密码行业标准。	2009	2011	2012	2016
1099	单项选择题	ZUC算法驱动部分LFSR反馈系数不包括（ ）。	2^{12}	2^{15}	2^{17}	2^{21}
1100	单项选择题	ZUC算法驱动部分LFSR的抽头位置不包括（ ）。	s15	s10	s7	s0
1101	单项选择题	ZUC算法比特重组BR层从上层LFSR寄存器单元抽取位置不包括（ ）。	s0	s5	s9	s12
1102	单项选择题	ZUC算法比特重组BR层主要使用了软件实现友好的（ ）操作。	比特级异或	字符串连接	比特级AND	比特级OR

1103	单项选择题	ZUC算法非线性函数F部分使用的两个线性变换L1，L2的设计与（ ）算法线性扩散层的设计思想相同/类似。	SM4	AES	PRESENT	PRINCE
1104	单项选择题	ZUC算法非线性函数F部分包含（ ）个记忆单元。	2	4	6	8
1105	单项选择题	ZUC算法密钥载入过程中除了装入种子密钥，还要使用（ ）个设定的15比特常数。	8	12	16	20
1106	单项选择题	ZUC算法非线性函数F部分所使用的S盒之一与（ ）算法的S盒仿射等价。	PRINCE	AES	DES	PRESENT
1107	单项选择题	ZUC算法非线性函数F部分使用的两个线性变换L1，L2的设计采用了（ ）运算。	右循环移位	左循环移位	比特串联结	有限域乘法
1108	单项选择题	ZUC算法非线性函数F部分输入、输出长度分别为（ ）。	96， 96	96， 64	96， 32	32， 32
1109	多项选择题	以ZUC算法为核心，成为3GPP LTE标准的算法为（ ）。	128EEA-3	128EIA-3	128UEA-3	128UIA-3
1110	多项选择题	3GPP LTE算法标准的3个核心算法为（ ）。	ZUC	DES	AES	SNOW 3G
1111	多项选择题	ZUC算法结构的核心部分包括（ ）。	LFSR	比特重组BR	非线性函数F	Feistel网络
1112	多项选择题	ZUC算法中使用到的运算包括（ ）。	模2^{31}-1的加法	模2^{32}的加法	右循环移位	左循环移位
1113	多项选择题	ZUC算法非线性函数F部分使用的非线性运算包括（ ）。	S-盒变换	模2^{32}的加法	模2^{31}-1的加法	比特串异或运算
1114	多项选择题	ZUC算法非线性函数F部分使用的两个线性变换L1，L2采用（ ）运算设计，降低了实现代价。	右循环移位	左循环移位	比特串异或运算	有限域乘法
1115	多项选择题	ZUC算法密钥装载时LFSR中需要装入（ ）。	种子密钥	初始向量	16个15比特常数	15个15比特常数
1116	多项选择题	关于ZUC算法初始化过程描述正确的是（ ）。	迭代64轮	初始化完成后直接输出密钥流	迭代32轮	非线性函数的输出会参与LFSR的反馈运算

1117	多项选择题	关于ZUC算法非线性函数F部分使用S盒描述正确的是（ ）。	仅使用2个S盒	采用8比特S盒	采用4比特S盒	使用4个S盒
1118	多项选择题	关于ZUC算法描述正确的是（ ）。	3GPP LTE唯一标准	基于素域上的LFSR设计	算法结构新颖	算法软硬件实现性能良好
1119	判断题	流密码的强度主要取决于密钥流生成器的设计。	正确	错误		
1120	单项选择题	一个同步流密码具有很高的密码强度主要取决于（ ）。	密钥流生成器的设计	密钥长度	明文长度	密钥复杂度
1121	单项选择题	序列密码也称为（ ），它是对称密码算法的一种。	非对称密码	公钥密码	流密码	古典密码
1122	单项选择题	如果序列密码所使用的是真正随机方式的、与消息流长度相同的密钥流，则此时的序列密码就是（ ）密码体制。	对称	非对称	古典	一次一密
1123	单项选择题	以下是序列密码或流密码算法的是（ ）。	SM2算法	SM3算法	SM4算法	ZUC算法
1124	多项选择题	下列不属于序列密码的是（ ）。	DES	ZUC	AES	ECC
1125	单项选择题	RC4是一个典型的基于（ ）数组变换的序列密码。	线性	非线性	同步	异步
1126	单项选择题	m序列是（ ）移位寄存器序列的简称。	最长线性	最短线性	最长非线性	最短非线性
1127	单项选择题	以下密码算法不属于序列密算法的是（ ）。	ZUC	RC4	A5	IDEA
1128	多项选择题	序列密码算法有（ ）。	ZUC	RC4	AES	DES
1129	多项选择题	基于祖冲之算法的完整性算法工作流程中的步骤有（ ）。	初始化	函数扩展	产生密钥流	计算MAC
1130	多项选择题	下列属于序列密码算法的是（ ）。	RC4	A5	SEAL	SNOW2.0
1131	多项选择题	自同步序列密码的特性是（ ）。	自同步序列	有限的错误传播	加解密速度较快	消除明文统计特性
1132	单项选择题	一个同步流密码具有很高的密码强度主要取决于（ ）。	密钥流生成器的设计	密钥长度	明文长度	密钥复杂度
1133	单项选择题	ZUC-256的设计目标是针对（ ）的应用环境下提供256比特的安全性。	3G	4G	5G	2G
1134	单项选择题	我国（ ）被采纳为新一代宽带无线移动通信系统(LTE)国际标准。	ZUC算法	SM2算法	SM3算法	SM4算法
1135	多项选择题	通过祖冲之序列密码算法，能实现信息的（ ）。	机密性	完整性	真实性	不可否认性

1136	判断题	采用Feistel结构的密码算法的加解密过程具有相似性。	正确	错误		
1137	判断题	SHA-1生成的杂凑值的长度为160比特~~bit~~。	正确	错误		
1138	判断题	SHA-1的输入消息分组长度为218比特~~bit~~。	正确	错误		
1139	判断题	SHA-1的输出值的长度为152比特~~bit~~。	正确	错误		
1140	判断题	SHA-256的输入消息以512比特bit的分组为单位处理。	正确	错误		
1141	判断题	SHA-256的输出为256bit的杂凑值。	正确	错误		
1142	判断题	SM3密码杂凑算法和SHA-256的消息字介入方式相同。	正确	错误		
1143	判断题	SM3密码杂凑算法和SHA-256都是MD结构。	正确	错误		
1144	判断题	SM3密码杂凑算法和SHA-256的压缩函数完全相同。	正确	错误		
1145	判断题	根据目前公开的分析结果，SM3密码杂凑算法的安全性高于SHA-1。	正确	错误		
1146	判断题	SM3密码杂凑算法中的P置换是线性运算。	正确	错误		
1147	判断题	SM3密码杂凑算法一共有2个置换函数。	正确	错误		
1148	判断题	SM3密码杂凑算法的消息扩展过程一共生成128个消息字。	正确	错误		
1149	判断题	生日攻击是一种密码学攻击手段，基于概率论中生日问题的数学原理。SM3密码杂凑算法可以抵抗生日攻击。	正确	错误		
1150	判断题	SM3密码杂凑算法的布尔函数输出2个字。	正确	错误		
1151	判断题	SM3密码杂凑算法的轮函数每次更新2个字。	正确	错误		
1152	判断题	SM3密码杂凑算法的前16轮使用全异或的布尔函数。	正确	错误		

1153	判断题	SM3密码杂凑算法可以用来加解密数据。	正确	错误		
1154	判断题	SM3密码杂凑算法不是单向函数。	正确	错误		
1155	判断题	SM3密码杂凑算法的字长为16比特。	正确	错误		
1156	判断题	SM3密码杂凑算法的前16轮采用非线性的布尔函数。	正确	错误		
1157	判断题	SM3密码杂凑算法不能用来做数据完整性检测。	正确	错误		
1158	多项选择题	下列选项中可能涉及密码杂凑运算的是( )。	消息机密性	消息完整性	消息鉴别码	数字签名
1159	多项选择题	密码杂凑算法的基本安全属性有（ ）。	抗碰撞攻击	抗原像攻击	抗第二原像攻击	抗多个碰撞攻击
1160	单项选择题	以下算法采用不可逆的数学运算的是（ ）。	RC4	IDEA	DES	MD5
1161	单项选择题	关于杂凑函数下列描述有错误的是（ ）。	杂凑函数的输入长度固定	杂凑函数的输出长度固定	杂凑函数可用于数字签名方案	杂凑函数可用于消息完整性机制
1162	多项选择题	MD5算法主要包括的步骤有（ ）。	附加填充位	初始化链接变量	分组处理	执行步函数
1163	判断题	SM3密码杂凑算法消息字的存储采用小端形式，左边为低有效位，右边为高有效位。	正确	错误		
1164	判断题	SM3密码杂凑算法的消息填充方式和SHA-256基本相同。	正确	错误		
1165	判断题	SM3密码杂凑算法中没有使用循环移位运算。	正确	错误		
1166	判断题	SM3密码杂凑算法的消息分组长度是256比特。	正确	错误		
1167	单项选择题	下面（ ）不是杂凑函数的主要应用。	文件完整性验证	数字签名	数据加密	身份鉴别协议
1168	单项选择题	SHA-1接收任何长度的输入消息，并产生长度为（ ）位的杂凑值。	64	160	512	128
1169	单项选择题	如果杂凑函数的函数值为64位，则对其进行生日攻击的代价为（ ）。	2^16	2^32	2^48	2^64

1170	单项选择题	对于一个给定的杂凑函数H，其单向性是指（ ）。	对于给定的杂凑函数H，找到满足H(x)=h 的 x 在计算上是不可行的	对于给定的分组 x，找到满足 x≠y 且 H(x)=H(y)的 y 在计算上是不可行的	找到任何满足H(x)=H(y)的(x，y)在计算上是不可行的	以上说法都不对
1171	单项选择题	MD5算法输出报文杂凑值的长度为（ ）。	120	128	144	160
1172	判断题	SM3密码杂凑算法的杂凑值长度是消息分组长度的一半。	正确	错误		
1173	单项选择题	SM3是（ ）算法。	分组密码	公钥密码	数字签名	密码杂凑函数
1174	单项选择题	SM3密码杂凑算法的链接变量长度为（ ）比特。	128	224	256	512
1175	单项选择题	SM3密码杂凑算法的压缩函数一共（ ）轮。	32	64	80	120
1176	单项选择题	SM3密码杂凑算法采用（ ）结构。	MD结构	Sponge结构	HAIFA结构	宽管道结构
1177	单项选择题	SM3密码杂凑算法的压缩函数一共有（ ）种不同的布尔函数。	2	3	4	5
1178	单项选择题	SM3密码杂凑算法的压缩函数的输入一共有（ ）比特。	256	512	768	1024
1179	单项选择题	SM3密码杂凑算法输入的最大消息长度不超过（ ）比特。	2^32	2^64	2^128	任意长度
1180	单项选择题	SM3密码杂凑算法的消息分组长度为（ ）比特。	256	512	768	1024
1181	单项选择题	SM3密码杂凑算法（ ）年公开发布的。	2010	2012	2015	2016
1182	单项选择题	SM3密码杂凑算法（ ）年被批准成为行业标准。	2010	2012	2015	2016
1183	单项选择题	SM3密码杂凑算法（ ）年被批准成为国家标准。	2010	2012	2015	2016
1184	单项选择题	SM3密码杂凑算法最少填充（ ）比特。	1	32	64	65
1185	单项选择题	SM3密码杂凑算法最多填充（ ）比特。	64	256	512	576
1186	单项选择题	SM3密码杂凑算法填充后消息的最短长度是（ ）比特。	0	256	512	1024

1187	单项选择题	SM3密码杂凑算法字的存储采用（ ）方式。	大端	小端	大小端混合	其他
1188	单项选择题	对输入为448比特的消息，SM3密码杂凑算法生成杂凑值时需要调用（ ）次压缩函数。	1	2	3	4
1189	单项选择题	SM3密码杂凑算法P0和P1置换中有（ ）个异或操作。	2	3	4	5
1190	单项选择题	SM3密码杂凑算法的字长是（ ）比特。	8	16	32	64
1191	单项选择题	SM3密码杂凑算法链接变量一共（ ）个消息字。	4	6	8	16
1192	单项选择题	SM3密码杂凑算法的布尔函数的输入有（ ）个消息字。	2	3	4	5
1193	单项选择题	SM3密码杂凑算法的消息扩展过程一共生成（ ）消息字。	64	128	132	256
1194	单项选择题	SM3密码杂凑算法不能用于（ ）方面。	消息源真实性鉴别	加解密数据	密钥生成	随机数生成
1195	单项选择题	SM3密码杂凑算法压缩函数中与当前内部状态进行计算时使用的操作是（ ）。	异或	模加	与运算	或运算
1196	单项选择题	SM3密码杂凑算法的初始值IV一共（ ）比特。	8	128	256	512
1197	单项选择题	SM3密码杂凑算法的P置换中有1比特输入差分，输出差分至少有（ ）比特。	1	2	3	9
1198	单项选择题	SM3密码杂凑算法的输入消息为“abc”，填充后的消息中，一共有（ ）个全“0”消息字。	8	10	12	14
1199	单项选择题	SM3密码杂凑算法的输入消息为“abcd”，填充后的消息中，一共有（ ）个非“0”32比特字。	1	2	3	4
1200	单项选择题	SM3密码杂凑算法最少填充（ ）比特“0”。	0	1	63	64
1201	多项选择题	以下关于SM3密码杂凑算法和SHA-256的描述正确的是（ ）。	消息字的介入方式相同	消息扩展过程生成的总消息字个数相同	杂凑值的长度相同	压缩函数的轮数

1202	多项选择题	SM3密码杂凑算法的压缩长度可以为（ ）比特。	2^32	2^48	2^64	任意长度
1203	多项选择题	SM3密码杂凑算法的运算中（ ）起到扩散的作用。	循环移位	P置换	模加	布尔函数
1204	多项选择题	SM3密码杂凑算法的运算中（ ）起到混淆的作用。	循环移位	P置换	模加	布尔函数
1205	多项选择题	以下关于SM3密码杂凑算法的描述正确的是（ ）。	SM3密码杂凑算法是我国密码行业标准算法	SM3密码杂凑算法是双管道杂凑函数	SM3密码杂凑算法是MD结构的杂凑函数	SM3密码杂凑算法的杂凑值长度和链接变量长度相同
1206	多项选择题	SM3密码杂凑算法能实现的功能有（ ）。	数字签名和验证	消息鉴别码的生成与验证	随机数的生成	加解密数据
1207	多项选择题	SM3密码杂凑算法的应用有（ ）。	口令保护	数字签名	数字证书	密钥派生
1208	多项选择题	以下（ ）算法不是密码杂凑函数。	MD5	AES	SM4	SM3
1209	多项选择题	以下（ ）操作是SM3密码杂凑算法的过程。	消息填充	迭代压缩	链接变量截取	生成杂凑值
1210	多项选择题	到目前为止，以下算法是安全的算法（不存在对算法的有效攻击）的是（ ）。	MD5	SHA-1	SHA-256	SM3
1211	多项选择题	杂凑算法又称密码散列、杂凑算法、摘要算法。到目前为止，以下算法是不安全的杂凑算法的有（ ）。	MD4	RIPEMD	SM3	SHA-0
1212	多项选择题	SM3密码杂凑算法的压缩函数的结构和（ ）算法相同。	MD5	SHA-3	SHA-1	SHA-256
1213	多项选择题	下列属于对密码杂凑函数的攻击方法是（ ）。	生日攻击	暴力破解攻击	已知明文攻击	选择密文攻击
1214	判断题	SM3密码杂凑算法的杂凑值长度和MD5的杂凑值长度相等。	正确	错误		
1215	判断题	SM3密码杂凑算法的杂凑值长度和SHA-256的杂凑值长度相等。	正确	错误		
1216	判断题	SM3密码杂凑算法是典型的轻量级杂凑函数。	正确	错误		
1217	判断题	SM3密码杂凑算法的杂凑值长度为160比特。	正确	错误		
1218	多项选择题	不能用于对消息鉴别码进行攻击的方法是（ ）。	重放攻击	字典攻击	查表攻击	选择密文攻击

1219	多项选择题	2004年8月，在美国加州圣芭芭拉召开的国际密码大会上，王小云教授首次宣布了她的研究成果，对（ ）等几种著名密码算法的破译结果。	MD5	SHA-1	AES	RSA
1220	单项选择题	输入消息“abcd”，经过SM3密码杂凑算法填充后，消息的最后32比特是（ ）。	0x00000001	0x00000020	0x80000001	0x80000020
1221	单项选择题	一个输出杂凑值长度为n比特的理想杂凑函数，原像攻击的复杂度是（ ）。	O(2^n)	O(2^(n/2))	O(2^(3n/4))	O(n)
1222	单项选择题	一个输出杂凑值长度为n比特的理想杂凑函数，碰撞攻击的复杂度是（ ）。	O(2^n)	O(2^(n/2))	O(2^(3n/4))	O(n)
1223	单项选择题	一个输出杂凑值长度为n比特的理想杂凑函数，第二原像攻击的复杂度是（ ）。	O(2^n)	O(2^(n/2))	O(2^(3n/4))	O(n)
1224	单项选择题	理想的Merkle-Damgård（MD）结构的杂凑函数不能有效抵抗的攻击有（ ）。	碰撞攻击	原像攻击	第二原像攻击	长度扩展攻击
1225	单项选择题	SM3密码杂凑算法中，输入消息“abc”的长度是（ ）比特。	3	4	24	32
1226	单项选择题	以下哪种密码杂凑算法的安全强度与SM3算法的安全强度相当（ ）。	SHA-224	SHA-512/224	SHA-256	SHA-384
1227	单项选择题	SM3算法中消息分组和输出杂凑值的长度分别是（ ）比特。	512，256	512，512	256,512	256,256
1228	单项选择题	MD5和SHA-1的输出杂凑值长度分别是（ ）比特。	80，128	128，160	128,192	160,192
1229	单项选择题	利用带盐杂凑方式对口令进行保护，利用的是密码杂凑算法的（ ）特性。	单向性	抗第二原像攻击	弱抗碰撞性	强抗碰撞性
1230	多项选择题	以下算法是杂凑函数的是（ ）。	SHA-256	SM3	Keccak	RC4
1231	多项选择题	属于杂凑函数的是（ ）。	SHA-1	MD2	DES	RC4
1232	多项选择题	密码杂凑算法的安全特性包括（ ）。	单向性	抗弱碰撞	抗强碰撞	抗伪造
1233	多项选择题	以下哪些参数的长度，与SM3的输入消息分组长度相同（ ）。	基于SM4产生的CBC-MAC值	HMAC-SM3产生的完整MAC值	RSA-512的签名值	SM2的公钥值

1234	判断题	MD5、SHA-1、SHA-256这3个算法所输出的杂凑值长度是不同的，而它们的分组长度也不同。	正确	错误		
1235	判断题	SHA-256和SHA-512输入消息的最大长度是相同的。	正确	错误		
1236	判断题	MD系列算法和SHA系列算法都是采用Merkle-Damgård（MD）迭代结构的。	正确	错误		
1237	判断题	杂凑函数是可逆的。	正确	错误		
1238	判断题	MD5算法的输出为128比特。	正确	错误		
1239	判断题	SM3算法每个分组的迭代轮数有32轮。	正确	错误		
1240	判断题	SHA-512的输出长度是512比特。	正确	错误		
1241	判断题	SHA-512以512位的分组为单位处理消息。	正确	错误		
1242	判断题	SHA-512处理消息时，每个分组有80轮运算。	正确	错误		
1243	判断题	HMAC计算过程中调用了2次杂凑函数。	正确	错误		
1244	判断题	使用Sponge结构的密码杂凑函数，输入的数据在进行填充之后，要经过吸收阶段和挤出阶段，最终生成输出的杂凑值。	正确	错误		
1245	判断题	MD5与SM3的杂凑值长度分别为128比特与256比特。	正确	错误		
1246	单项选择题	SM3 密码杂凑算法中生成杂凑值的长度为（ ）比特。	32	64	128	256
1247	单项选择题	密码杂凑函数（Hash函数）按照是否使用密钥分为两大类：带密钥的杂凑函数和不带密钥的杂凑函数，下面算法中属于带密钥的杂凑函数的是（ ）。	MD4	SHA-1	HMAC	MD5
1248	单项选择题	请从下列各项中选出不是加密算法的选项（ ）。	MD5算法	AES算法	SM4算法	DES算法

1249	单项选择题	如果杂凑函数的杂凑值为128位，则对其进行生日攻击的复杂度为（　）。	2的32次方	2的64次方	2的56次方	2的128次方
1250	单项选择题	如果杂凑函数的杂凑值为256位，则对其进行生日攻击的复杂度为（　）。	2的32次方	2的64次方	2的56次方	2的128次方
1251	单项选择题	MD5杂凑值算法输出的长度为（　）。	64位	128位	32位	不固定
1252	单项选择题	在SM3算法中，分组长度为（　）位。	56	64	488	512
1253	多项选择题	关于HMAC的说法正确的是（　）。	验证收到的消息的完整性和真实性	SSL中使用了HAMC	要求使用密钥	基于杂凑函数设计的
1254	多项选择题	下列属于杂凑函数的是（　）。	MD5	SHA-1	SM3	SM2
1255	多项选择题	下面关于SHA-1的附加填充位操作，说法正确的是（　）。	填充一个1和若干个0	在消息后附加32bit的无符号整数	长度模512与448同余	填充后的消息长度为512比特的整数倍
1256	判断题	SM3密码杂凑算法在2018年10月正式成为ISO/IEC国际标准。	正确	错误		
1257	判断题	杂凑函数可以用分组密码算法来构造。	正确	错误		
1258	判断题	杂凑函数可以用于构造伪随机数生成器。	正确	错误		
1259	判断题	SM3密码杂凑算法的杂凑值长度是256比特。	正确	错误		
1260	多项选择题	以下哪项是杂凑函数功能（ ）。	不能逆向执行	提供了消息的完整性	单向哈希的结果是报文杂凑值	提供了消息的保密性
1261	多项选择题	以下关于杂凑算法的说法，正确的是（ ）。	单向散列函数是数字签名的一个关键环节，可以大大缩短签名时间	单向散列函数可以分为两类：带密钥的单向散列函数和不带密钥的单向散列函数	HMAC是实现MAC的算法，在Internet上广泛使用的安全套接层（SSL）协议中使用	MD5和SHA-1是杂凑算法

1262	多项选择题	单向杂凑函数可以用于以下哪些方面（ ）。	数字签名	密钥共享	消息完整性检测	操作系统中账号口令的安全存储
1263	多项选择题	理想MD结构的杂凑函数能有效抵抗的攻击有（ ）。	碰撞攻击	原像攻击	多碰撞攻击	长度扩展攻击
1264	多项选择题	以下属于MD5算法过程的是（ ）。	附加信息填充位	初始化链接变量	迭代压缩	执行步函数
1265	多项选择题	下列关于SHA-3的说法正确的是（ ）。	SHA-3是基于Sponge结构设计的	不限定输入消息的长度	输出消息的长度根据需要可变	适用于SHA-1 的攻击方法也可以作用于SHA-3
1266	多项选择题	下列关于杂凑函数的说法正确的是（ ）。	杂凑函数是可逆的	杂凑函数具有强抗碰撞性	杂凑函数具有弱抗碰撞性	杂凑函数是一种具有压缩特性的函数
1267	判断题	SM3密码杂凑算法的杂凑值长度是128比特。	正确	错误		
1268	判断题	SM3密码杂凑算法采用MD迭代结构。	正确	错误		
1269	判断题	SM3密码杂凑算法的初始值长度和杂凑值长度不相同。	正确	错误		
1270	单项选择题	下面算法运算时不需要密钥的是（ ）。	SM2	SM4	ZUC	SM3
1271	多项选择题	根据杂凑函数的安全水平，人们将杂凑函数分为两大类，分别是（ ）。	弱碰撞自由的杂凑函数	强碰撞自由的杂凑函数	强杂凑函数	弱杂凑函数
1272	多项选择题	下列不属于SHA-3杂凑算法结构的是（ ）。	MD结构	非平衡的Feistel结构	平衡的Feistel结构	Sponge结构
1273	多项选择题	下面属于杂凑函数主要应用的是（ ）。	文件校验	数字签名	数据加密	认证协议
1274	多项选择题	攻击杂凑函数的方法有（ ）。	穷举攻击法	生日攻击	中途相遇攻击	伪造攻击
1275	多项选择题	杂凑函数满足的条件有（ ）。	函数的输入可以是任意长	函数的输出是固定长	已知x，求H(x)较为容易，可用硬件或软件实现	找出任意两个不同的输入x、y，使得H(y)=H(x)在计算上是不可行的

1276	判断题	单向陷门函数，是在不知陷门信息的情况下求逆困难的函数，当知道陷门信息后，求逆是易于实现的。	正确	错误		
1277	多项选择题	杂凑算法的基本安全属性有（ ）。	抗碰撞攻击	抗原像攻击	抗第二原像攻击	抗多碰撞个攻击
1278	判断题	MD5是最强的加密算法，可以有效防止不安全的加密存储。	正确	错误		
1279	单项选择题	在公钥密码体制中，加密过程中用（ ）。	对方的公钥	自己的公钥	自己的私钥	用公钥和私钥
1280	单项选择题	RSA公钥密码算法的安全性基于（ ）。	模指数计算	离散对数求解问题	数论中大整数分解的困难性	Euler定理
1281	单项选择题	ElGamal公钥密码体制的安全性基于（ ）。	数域上的离散对数问题	椭圆曲线上的离散对数问题	数域上大整数素数分解问题	椭圆曲线上大整数素数分解问题
1282	单项选择题	利用RSA公钥密码体制（OAEP填充模式）两次加密相同的明文，密文（）。	不同	相同	有时相同，也有不同	根据具体情况
1283	单项选择题	利用SM2公钥密码体制两次加密相同的明文，密文（）。	不同	相同	有时相同，也有不同	根据具体情况
1284	多项选择题	公钥密码算法使用两个密钥，下述描述正确的是（ ）。	一个是公钥，一个是私钥	一个是加密密钥，一个是解密密钥	一个是公开的密钥，一个是秘密保存的私钥	一个用于加密，一个用于MAC
1285	单项选择题	下述（ ）密码算法与SM2算法使用相同的数学难题。	AES	RSA	ECDSA	DES
1286	多项选择题	SM2算法与（ ）算法属于同一类数学结构。	ECDH	RSA	ECDSA	SM9
1287	单项选择题	SM2算法的安全性基于（ ）困难假设。	双线性映射	椭圆曲线离散对数	多线性映射	丢番图方程求解
1288	单项选择题	SM2算法是（ ）商用密码算法。	美国	中国	欧盟	俄罗斯
1289	多项选择题	下列密码体制不是基于多变量公钥密码的是（ ）。	AES	DES	RSA	ElGamal
1290	多项选择题	下列密码体制的安全性是基于大整数分解问题的是（ ）。	RSA	ECC	Rabin	ElGamal
1291	多项选择题	下列密码体制的安全性是基于离散对数问题的是（ ）。	RSA	Rabin	SM2	ElGamal

1292	多项选择题	根据所依据的数学难题，公钥密码体制可以分为以下几类（ ）。	模幂运算问题	大整数因子分解问题	有限域离散对数问题	椭圆曲线离散对数问题
1293	多项选择题	SM2的安全特性主要体现在（ ）方面。	算法具备单向性	密文不可区分性	密文具有抗碰撞性	密文具有不可延展性
1294	单项选择题	测评过程中，可以作为可能使用SM2加密的证据有（ ）。	密文比明文长64个字节	密文的第一部分是SM2椭圆曲线上的点	密文长度为512比特	加密公钥长度为256比特
1295	判断题	SM2与SM9都是基于椭圆曲线设计的密码算法。	正确	错误		
1296	判断题	SM2算法可用于数字签名、密钥交换、公钥加密。	正确	错误		
1297	单项选择题	我国商用密码算法SM2是一种椭圆曲线公钥密码算法，其推荐的密钥长度为（ ）。	128比特	256比特	192比特	512比特
1298	多项选择题	以下（ ）是SM9的应用场景。	密钥封装	协商密钥	加密数据	数字签名
1299	单项选择题	目前公钥密码主要用来进行数字签名，或用于保护传统密码的密钥，而不主要用于数据加密，主要因为（ ）。	公钥密码的私钥太长	公钥密码的效率比较低	公钥密码的安全性不好	公钥密码抗攻击性比较差
1300	单项选择题	多变量公钥密码的安全性基础是基于（ ）的困难性。	求解有限域上随机生成的多变量非线性多项式方程组	大整数分解	任意线性码的译码问题	最小整数解问题
1301	多项选择题	公钥密码体制的出现，解决了对称密码体制很难解决的一些问题。主要体现在（ ）。	密钥分发	密钥管理	一次一密	抗抵赖
1302	多项选择题	相对于对称加密算法，非对称密钥加密算法通常( )。	加密速率较低	更适合于数据的加解密处理	安全性一定更高	加密和解密的密钥不同
1303	单项选择题	RSA密码算法的安全性是基于（ ）。	离散对数问题的困难性	子集和问题的困难性	大整数因子分解的困难性	线性编码的解码问题的困难性
1304	单项选择题	Alice收到Bob发给她的一个文件的签名，并要验证这个签名的有效性，那么签名验证算法需要Alice选用的密钥是（ ）。	Alice的公钥	Alice的的私钥	Bob的公钥	Bob的私钥

1305	单项选择题	公钥密码学的思想最早是由（ ）提出的。	欧拉（Euler）	迪菲（Diffie）和赫尔曼（Hellman）	费马（Fermat）	里维斯特（Rivest）、沙米尔（Shamir）和埃德蒙（Adleman）
1306	单项选择题	PKI主要基于的密码体制是（ ）。	对称密码	公钥密码	量子密码	密码杂凑算法
1307	多项选择题	公钥密码中，密钥可以分为（ ）。	主密钥	公钥	私钥	会话密钥
1308	多项选择题	下列密码体制的安全性是基于大整数分解问题的是（ ）。	ECC	RSA	Rabin	ElGamal
1309	多项选择题	下列属于对RSA攻击的方法有（ ）。	共模攻击	广播攻击	因式分解	字典攻击
1310	多项选择题	以下不是背包公钥加密体制的是（ ）。	LWE	ECC	Merkle-Hellman	McEliece
1311	判断题	SM9是基于标识的密码算法。	正确	错误		
1312	判断题	SM9密码算法的主公钥由KGC通过随机数发生器产生。	正确	错误		
1313	判断题	SM9密码算法的用户私钥由KGC通过随机数发生器产生。	正确	错误		
1314	判断题	SM9密码算法使用256位的BN曲线。	正确	错误		
1315	判断题	SM9密码算法的密钥派生函数需要调用Hash函数。	正确	错误		
1316	判断题	SM9密码算法的消息认证码函数需要调用Hash函数。	正确	错误		
1317	判断题	椭圆曲线双线性对的安全性是SM9密码算法安全性的重要基础。	正确	错误		
1318	判断题	SM9密码算法需要保证选取的椭圆曲线上离散对数问题难解。	正确	错误		
1319	判断题	在采用SM9数字签名算法生成/验证签名之前，需要使用Hash函数对待签/待验证消息进行压缩。	正确	错误		
1320	判断题	SM9密钥封装机制封装的秘密密钥由解封装用户使用主私钥进行解密。	正确	错误		
1321	判断题	SM9公钥加密算法是密钥封装机制和消息封装机制的结合。	正确	错误		

1322	判断题	SM9公钥加密算法消息封装机制使用了KDF作为辅助函数。	正确	错误		
1323	判断题	根据SM9标识密码算法行业标准的规定，SM9密码算法使用的Hash函数必须是SM3算法。	正确	错误		
1324	判断题	根据SM9标识密码算法行业标准的规定，SM9密码算法必须使用国家密码管理主管部门批准的随机数发生器。	正确	错误		
1325	判断题	根据SM9标识密码算法行业标准的规定，SM9密码算法使用的分组密码算法必须是SM4算法。	正确	错误		
1326	判断题	SM9密码算法采用的椭圆曲线嵌入次数越大安全性越高，因此嵌入次数越大越好。	正确	错误		
1327	判断题	SM9密码算法椭圆曲线点的字节串表示形式有3种：压缩、未压缩和混合表示形式。	正确	错误		
1328	判断题	SM9是分组密码算法。	正确	错误		
1329	判断题	SM9是序列密码算法。	正确	错误		
1330	判断题	SM9是Hash算法。	正确	错误		
1331	判断题	SM9密码算法采用的椭圆曲线双线性对是R-ate对。	正确	错误		
1332	单项选择题	在现有的计算能力条件下，ElGamal算法的最小密钥长度是（ ）。	128位	160位	512位	1024位
1333	单项选择题	Bob给Alice发送一封邮件，为让Alice确信邮件是由Bob发出的，则Bob应该选用（ ）对邮件签名。	Alice的公钥	Alice的私钥	Bob的公钥	Bob的私钥
1334	单项选择题	利用公钥加密和私钥解密的密码体制是（ ）。	对称加密体制	非对称加密体制	轴对称加密体制	空间对称加密体制
1335	单项选择题	下列的加密方案基于格理论的是（ ）。	ECC	RSA	AES	Regev
1336	多项选择题	下列属于后量子公钥密码研究方向的是（ ）。	多变量公钥密码	基于格的公钥密码	基于纠错码的公钥密码	基于椭圆曲线离散对数困难问题的公钥密码

1337	多项选择题	关于公钥密码体制以下选项中正确的是（ ）。	公钥加密体制用私钥加密	公钥密码体制用公钥加密	公钥密码体制用私钥签名	公钥密码体制的公钥和私钥相同
1338	单项选择题	SM2算法中的（ ）算法已经进入ISO国际标准。	数字签名	公钥加密	密钥交换	身份认证
1339	单项选择题	SM2算法中的密钥交换算法支持（ ）方密钥交换。	2	3	4	多
1340	单项选择题	基域选择256比特素域时，SM2算法的数字签名的长度为（ ）比特。	128	256	384	512
1341	单项选择题	关于RSA公钥算法，下列说法错误的是（ ）。	RSA加密算法中，公钥为（n,e）	RSA加密算法中，公钥e与ϕ(n)互素	同等安全强度下，RSA签名速度比ECC算法快	RSA加密速度比解密速度快
1342	单项选择题	RSA-3072 with SHA-224的安全强度为（ ）比特。	80	112	128	192
1343	判断题	SM9数字签名算法的辅助函数包括密码杂凑函数和随机数发生器。	正确	错误		
1344	判断题	SM9密钥封装机制和公钥加密算法都需要密钥派生函数作为辅助函数。	正确	错误		
1345	判断题	SM9密钥交换协议要求必须有密钥确认。	正确	错误		
1346	判断题	SM9密码算法的标识可以是姓名、性别、年龄、身份证号、手机号码中的一种。	正确	错误		
1347	判断题	SM9密码算法用户标识由KGC生成。	正确	错误		
1348	判断题	SM9密钥封装机制封装的秘密密钥是根据解封装用户的标识生成的。	正确	错误		
1349	判断题	SM9密码算法系统参数由KGC选择。	正确	错误		
1350	判断题	SM9数字签名算法签名者使用主私钥生成签名，验证者使用主公钥进行验证。	正确	错误		
1351	判断题	SM9公钥加密算法使用接受者的用户标识加密数据，使用接受者私钥对数据进行解密。	正确	错误		

1352	判断题	SM9密钥交换协议需要使用密码杂凑函数、密钥派生函数、随机数发生器作为辅助函数。	正确	错误		
1353	判断题	SM9数字签名算法、密钥交换协议、密钥封装机制、公钥加密算法都需要使用密码杂凑函数和随机数发生器作为辅助函数。	正确	错误		
1354	判断题	SM9公钥加密算法中消息认证码函数使用密钥派生函数生成的密钥。	正确	错误		
1355	单项选择题	SM2数字签名算法无法实现的功能是（ ）。	数据来源确认	消息机密性	签名者不可抵赖	数据完整性验证
1356	单项选择题	SM2算法中计算量最大的运算是（ ）。	椭圆曲线点加	椭圆曲线倍点	椭圆曲线点乘	杂凑
1357	单项选择题	SM2算法基于的椭圆曲线离散对数的计算复杂度为（ ）。	指数级	亚指数级	超指数级	超多项式
1358	单项选择题	SM2算法采用的素域椭圆曲线构成的数学结构是（ ）。	交换群	非交换群	环	域
1359	单项选择题	SM2算法采用的素域椭圆曲线的基本参数不包括（ ）。	域的规模	基点的阶	基点	无穷远点
1360	单项选择题	SM2算法基于的椭圆曲线上的点乘计算的计算复杂度为（ ）。	线性级	多项式级	超多项式级	亚指数级
1361	单项选择题	SM2算法采用的椭圆曲线上的无穷远点是群的（ ）点。	0	最大点	基点	1
1362	单项选择题	SM2算法公开参数中的基点是（ ）。	椭圆曲线群的0点	椭圆曲线群的生成元	椭圆曲线群的最大点	基域的生成元
1363	单项选择题	SM2算法中的公钥加密算法的公钥是（ ）。	基域的元素	椭圆曲线上的随机点	椭圆曲线的0点	椭圆曲线的基点
1364	单项选择题	ECDH密钥交换算法中单个用户需要计算（ ）次点乘运算。	1	2	3	4
1365	单项选择题	SM2算法的数字签名的签名值包含（ ）部分。	2	3	4	1
1366	单项选择题	SM2公钥加密算法的密文值包含（ ）部分。	1	2	3	4
1367	单项选择题	ECDSA公钥加密算法无法抵抗的攻击有（ ）。	密钥恢复攻击	唯密文攻击	选择明文攻击	量子计算攻击
1368	单项选择题	SM2公钥加密算法的公钥包含（ ）个椭圆曲线上的点。	1	2	3	4

1369	单项选择题	SM2算法中的数字签名算法的签名函数包含（ ）次点乘运算。	1	2	3	4
1370	单项选择题	SM2算法中的数字签名的签名运算最耗时的是（ ）运算。	随机数生成	消息映射	素性检测	点乘
1371	单项选择题	基域选择Fp-256时，SM2算法的数字签名的私钥长度为（ ）。	128	256	384	512
1372	单项选择题	基域选择Fp-256时，SM2算法的数字签名的公钥长度为（ ）。	128	256	384	512
1373	单项选择题	基域选择Fp-256时，SM2公钥加密算法的私钥长度为（ ）。	128	256	384	512
1374	单项选择题	SM2密码算法的安全强度大致相当于（ ）比特长度的RSA算法。	1024	2048	3072	4096
1375	单项选择题	若一个SM2公钥表示为（x，y），那么该公钥可以压缩为（ ）。	x分量，以及y分量的最高位	x分量，以及y分量的最低位	x分量的最高位，以及y分量	x分量的最低位，以及y分量
1376	单项选择题	用SM2算法实现一个对1024比特明文的加密，需要（ ）次点乘运算。	1	2	4	8
1377	单项选择题	如果明文长度是128比特，那么经过SM2加密后的密文长度是（ ）。	128比特	256比特	896比特	1024比特
1378	单项选择题	下列哪个标准定义了SM2算法的密钥数据格式、加密数据格式、签名数据格式以及密钥对保护数据的格式等（ ）。	GM/T 0003 SM2椭圆曲线公钥密码算法	GM/T 0009 SM2密码算法使用规范	GM/T 0010 SM2密码算法加密签名消息语法规范	GM/T 0015 基于SM2密码算法的数字证书格式规范
1379	单项选择题	如果SM2的密文长度是2048比特，那么相应明文长度是（ ）比特。	1024	1280	2048	2816
1380	单项选择题	（ ）算法使用同一个私钥对同一个消息签名后，签名值始终一致，即该算法是一个确定性签名算法。	SM2签名	RSA-PKCS1-v1_5签名	RSA-PSS签名	ECDSA
1381	单项选择题	下列不属于SM2公钥加密算法特点的是（ ）。	每次加密数据时，引入不同的随机数	可用于产生数字信封	解密过程可以验证结果正确性	密文比明文长64字节
1382	多项选择题	非对称密码体制可实现数据的（ ）。	机密性	完整性	真实性	不可抵赖性
1383	多项选择题	关于椭圆曲线密码体制正确的是（ ）。	运算速度一般比对称密码算法快	运算速度一般比对称密码慢	密钥长度一般比同等强度的RSA短	密钥长度一般比同等强度的RSA长

1384	多项选择题	关于RSA的参数选择，正确的是（ ）。	选取两个秘密素数p和q	选取两个公开素数p和q	（p-1）和（q-1）都必须至少具有一个很大的素因数	p和q二者之差不宜过小
1385	多项选择题	公钥加密，也叫非对称（密钥）加密。以下属于公钥密码算法的是（ ）。	MD4	RSA	ECC	ElGamal
1386	多项选择题	相对于对称密码算法，公钥密码算法的特点是（ ）。	加密速度慢	更适合于批量数据加解密处理	加密速度快	加密和解密的密钥不同
1387	多项选择题	SM2算法涉及到的数据格式包括（ ）。	椭圆曲线点	有限域元素	比特串	字符串
1388	多项选择题	SM2公钥加密算法可以抵抗的攻击包括（ ）。	唯密文攻击	选择明文攻击	选择密文攻击	密钥恢复攻击
1389	多项选择题	由国内学者提出的算法标准包括（ ）。	NTRU	ZUC	SM4	SM2
1390	多项选择题	基于椭圆曲线数学结构的算法包括（ ）。	SM9	SM2	SM3	NTRU
1391	多项选择题	离散对数问题是一个在数学和密码学领域中的重要问题。基于离散对数问题的密码算法包括（ ）。	RSA	SM2	ECDSA	NTRU
1392	多项选择题	SM2公钥加密算法的加密函数涉及到的运算有（ ）。	随机数生成	杂凑值计算	椭圆曲线点乘	KDF
1393	多项选择题	SM2公钥加密算法的密文包含的元素有（ ）。	椭圆曲线点	杂凑值	比特串	域元素
1394	多项选择题	以下说法正确的是（ ）。	RSA算法加密速度比解密速度快	RSA算法加密速度比解密速度慢	RSA算法签名速度比验签速度快	RSA算法签名速度比验签速度慢
1395	多项选择题	SM2公钥密码算法一般包括如下哪些功能（ ）。	密钥派生	签名	密钥交换	加密
1396	多项选择题	以下关于SM9算法与SM2算法的描述正确的是（ ）。	基于的困难问题略有不同	SM9的私钥均需要由密钥管理中心生成，用户自己无法产生	SM2的私钥产生可以不需要密钥管理中心的参与	SM9使用时不需要数字证书实现实体与公钥的绑定

1397	多项选择题	A利用B的SM2公钥直接加密消息，将SM2密文传输给B，以下说法正确的是（ ）。	这种方式可以实现消息源真实性鉴别	这种方式不常用，SM2一般用于加密一个对称加密密钥	这种方式可以对消息的机密性进行保护	这种方式可以防范对消息的恶意替换
1398	多项选择题	SM2签名结果用ASN.1 DER表示时，如果签名值为71字节，可能的情形是（ ）。	签名值中，r的最高位为1，s的最高位为0	签名值中，r的最高位为0，s的最高位为1	签名值中，r的最高位为0，s的最高位为0	签名值中，r的最高位为1，s的最高位为1
1399	多项选择题	有关SM9标识密码算法描述错误的是（ ）。	用户的公钥由用户标识唯一确定，用户需要通过第三方保证其公钥的真实性	SM9密钥交换协议可以使通信双方通过对方的标识和自身的私钥经2次或可选3次信息传递过程，计算获取一个由双方共同决定的共享秘密密钥	SM9密码算法的用户公钥长度一定为512比特，算法的应用与管理不需要数字证书	在基于标识的加密算法中，解密用户持有一个标识和一个相应的私钥，该私钥由密钥生成中心通过主私钥和解密用户的标识结合产生。加密用户用解密用户的标识加密数据，解密用户用自身私钥解密数据
1400	判断题	IBC信任体系中，用户签名私钥既可以自己产生，也可以统一由密钥生成中心KGC产生。	正确	错误		
1401	判断题	SM2、SM9算法私钥值需大于椭圆曲线群的阶。	正确	错误		
1402	判断题	在实际应用，RSA的加密过程是直接使用公钥对原始消息直接进行模幂计算。	正确	错误		
1403	判断题	由于随机数的引入，即便使用同一公钥对同一消息加密，SM2密文每次都是随机的。	正确	错误		
1404	判断题	为方便验签，SM2算法签名过程中使用的随机值k可选择公开。	正确	错误		
1405	判断题	SM2签名速率一般大于验签速率。	正确	错误		

1406	单项选择题	在RSA公钥密码算法中，设Φ(n)为欧拉函数，则Φ(77)的值为（ ）。	63	60	48	49
1407	单项选择题	椭圆曲线ECC中最关键的运算是（ ）。	倍点运算	矩阵加法运算	矩阵乘法运算	方程运算
1408	单项选择题	公钥密码的安全性理论基础是计算复杂性理论，其产生的最主要原因是（ ）。	简化密钥管理	加密算法简短	模运算	更安全
1409	单项选择题	公钥密钥密码体制往往基于一个（ ）。	平衡布尔函数	杂凑函数	单向函数	陷门单向函数
1410	单项选择题	RSA 、ElGamal 及McEliecc 公钥密码算法的安全性基础依次是（ ）。	计算离散对数的困难性、一般线性纠错码的困难性及分解大整数的困难性	计算离散对数的困难性、分解大整数的困难性及一般线性纠错码的困难性	分解大整数的困难性、计算离散对数的困难性及一般线性纠错码的困难性	分解大整数的困难性、一般线性纠错码的困难性及计算离散对数的困难性
1411	单项选择题	SM2标准中规定采用（ ）比特的椭圆曲线域参数。	128	192	256	512
1412	单项选择题	关于RSA公钥密码体制、ElGamal公钥密码体制、ECC公钥密码体制，下列描述正确的是（ ）。	如果密码体制参数不变，且不考虑填充的问题，明文和密钥一定时，则每次RSA加密的密文一定相同	如果明文和密钥一定时，则每次ECC加密的密文一定相同	如果明文和密钥一定时，则每次ElGamal加密的密文一定相同	以上都不对
1413	多项选择题	公钥密码的安全性理论基础是计算复杂性理论，如下哪些算法属于公钥密码算法（ ）。	SM2算法	SM9算法	RSA算法	SM3算法
1414	判断题	SM2是我国商用公钥密码算法标准，是基于椭圆曲线的公钥密码算法。	正确	错误		
1415	单项选择题	SM9是一种（ ）算法。	序列密码	分组密码	公钥密码	杂凑函数
1416	单项选择题	SM9是一种（ ）的公钥密码算法。	基于格	基于编码	基于多变量	基于椭圆曲线双线性对
1417	单项选择题	（ ）是SM9密码算法的特点。	基于数字证书	抗量子计算攻击	基于标识	安全性基于大数分解问题难解性

1418	单项选择题	在（ ）年，中国国家密码管理局将SM9密码算法正式发布为密码行业标准。	2014	2015	2016	2017
1419	单项选择题	在（ ）年，SM9数字签名算法被一致通过为ISO/IEC国际标准，正式进入标准发布阶段。	2014	2015	2016	2017
1420	单项选择题	以下（ ）不能作为SM9密码算法的标识。	姓名	身份证号	手机号码	电子邮箱
1421	单项选择题	SM9密钥交换协议的辅助函数不包括（ ）。	杂凑函数	密钥派生函数	随机数发生器	分组密码算法
1422	单项选择题	（ ）算法是基于标识的密码算法。	SM2	SM3	SM4	SM9
1423	单项选择题	SM9密码算法系统参数不包括（ ）。	椭圆曲线方程参数	私钥生成函数识别符	椭圆曲线识别符	双线性对识别符
1424	单项选择题	SM9密码算法椭圆曲线无穷远点的字节串表示形式是（ ）。	单一零字节表示形式	压缩表示形式	未压缩表示形式	混合表示形式
1425	单项选择题	关于SM9密码算法选用椭圆曲线的嵌入次数说法正确的是（ ）。	嵌入次数越大安全性越高	嵌入次数越大双线性对计算越容易	选择椭圆曲线的嵌入次数越大越好	选择椭圆曲线的嵌入次数越小越好
1426	单项选择题	SM9密码算法采用的椭圆曲线双线性对是（ ）。	Weil对	Tate对	Ate对	R-ate对
1427	单项选择题	SM9密码算法采用的椭圆曲线的嵌入次数是（ ）。	10	11	12	13
1428	单项选择题	（ ）算法可用于做SM9数字签名算法的辅助函数。	SM1	SM2	SM3	SM4
1429	单项选择题	SM9数字签名的生成会用到（ ）。	主公钥	主私钥	标识	数字证书
1430	单项选择题	SM9密码算法主公钥由（ ）产生。	KGC通过随机数发生器	KGC通过主私钥结合系统参数	用户通过随机数发生器	用户通过主私钥结合系统参数
1431	单项选择题	SM9密码算法主私钥由（ ）产生。	KGC通过随机数发生器	KGC通过主公钥结合系统参数	用户通过随机数发生器	用户通过主公钥结合系统参数
1432	单项选择题	SM9密码算法用户私钥由（ ）产生。	KGC通过随机数发生器	KGC通过主私钥结合用户标识	用户通过随机数发生器	用户通过主私钥结合用户标识

1433	单项选择题	SM9密码算法用户公钥（ ）。	通过随机数发生器生成	根据用户标识唯一确定	通过主私钥结合系统参数生成	通过用户私钥结合系统参数生成
1434	单项选择题	SM9密码算法的功能不包括（ ）。	数字签名	密钥交换	杂凑函数	公钥加密
1435	单项选择题	在SM9数字签名的生成和验证过程之前，杂凑函数（ ）。	仅对待签名消息进行压缩	仅对待验证消息进行压缩	对待签名消息和待验证消息都要压缩	不起任何作用
1436	单项选择题	SM9密钥封装机制封装的秘密密钥是（ ）生成的。	根据主公钥	根据接受者的用户标识	由随机数发生器	以上都不对
1437	单项选择题	以下（ ）算法可以提供数字签名功能。	SM1	SM3	SM4	SM9
1438	单项选择题	以下（ ）算法可以提供密钥封装功能。	SM1	SM3	SM4	SM9
1439	单项选择题	以下（ ）算法可以提供公钥加密功能。	SM1	SM3	SM4	SM9
1440	多项选择题	SM9密码算法的主要内容包括（ ）。	数字签名算法	密钥交换协议	密钥封装机制	公钥加密算法
1441	多项选择题	SM9密码算法KGC是负责（ ）的可信机构。	选择系统参数	生成主密钥	生成用户标识	生成用户私钥
1442	多项选择题	SM9数字签名算法的辅助函数包括（ ）。	杂凑函数	密钥派生函数	随机数发生器	分组密码算法
1443	多项选择题	（ ）问题的难解性是SM9密码算法安全性的重要基础。	双线性逆	判定性双线性逆	τ-双线性逆	τ-Gap-双线性逆
1444	多项选择题	SM9密码算法涉及的数据类型有（ ）。	比特串	字节串	有限域元素	椭圆曲线上的点
1445	多项选择题	截至2017年底，（ ）没有被ISO/IEC通过为国际标准。	SM2数字签名算法	SM2密钥交换协议	SM9数字签名算法	SM9密钥交换协议
1446	多项选择题	SM9密码算法椭圆曲线非无穷远点的字节串表示形式有（ ）。	单一零字节表示形式	压缩表示形式	未压缩表示形式	混合表示形式
1447	多项选择题	（ ）算法用于SM9密码算法的辅助函数。	SM1	SM2	SM3	SM4

1448	多项选择题	关于SM9密码算法涉及的辅助函数以下说法正确的是（ ）。	根据SM9标识密码算法行业标准的规定，SM9密码算法使用的杂凑函数必须是SHA-256算法	根据SM9标识密码算法行业标准的规定，SM9密码算法使用的杂凑函数必须是国家密码管理主管部门批准的杂凑函数	根据SM9标识密码算法行业标准的规定，SM9密码算法使用的分组密码算法必须是AES算法	根据SM9标识密码算法行业标准的规定，SM9密码算法使用的分组密码算法必须是国家密码管理主管部门批准的分组密码算法
1449	多项选择题	杂凑函数和随机数发生器是（ ）算法的辅助函数。	SM9数字签名	SM9密钥交换	SM9密钥封装	SM9公钥加密
1450	多项选择题	密钥派生函数是（ ）算法的辅助函数。	SM9数字签名	SM9密钥交换	SM9密钥封装	SM9公钥加密
1451	多项选择题	SM9密码算法的特点有（ ）。	抗量子计算攻击	基于椭圆曲线双线性对	基于标识	基于数字证书
1452	多项选择题	SM9密码算法的标识可以有（ ）。	性别	电子邮箱	年龄	手机号码
1453	多项选择题	（ ）算法需要杂凑函数作为辅助函数。	SM9数字签名	SM9密钥交换	SM9密钥封装	SM9公钥加密
1454	多项选择题	（ ）算法需要随机数发生器作为辅助函数。	SM9数字签名	SM9密钥交换	SM9密钥封装	SM9公钥加密
1455	多项选择题	（ ）算法需要密钥派生函数作为辅助函数。	SM9数字签名	SM9密钥交换	SM9密钥封装	SM9公钥加密
1456	多项选择题	（ ）算法不需要消息鉴别码函数作为辅助函数。	SM9数字签名	SM9密钥交换	SM9密钥封装	SM9公钥加密
1457	多项选择题	（ ）算法不需要分组密码算法作为辅助函数。	SM9数字签名	SM9密钥交换	SM9密钥封装	SM9公钥加密
1458	判断题	具有64位长度密钥的RSA是绝对安全，不可以被破译的。	正确	错误		
1459	判断题	RSA体制的安全性是基于大整数因式分解问题的难解性。	正确	错误		
1460	判断题	RSA体制的安全性是基于离散对数问题。	正确	错误		
1461	判断题	ELGamal密码体制的安全性是基于离散对数问题。	正确	错误		
1462	判断题	在公钥密码体制中，密钥的秘密性不需要保护。	正确	错误		

1463	单项选择题	GM/T 0009《SM2密码算法使用规范》中，使用SM2密码算法对数据进行加密的过程内部中调用了（ ）密码算法。	SM7	SM4	SM3	ZUC
1464	单项选择题	消息鉴别码与数字签名的共同特点是（ ）。	保护数据机密性	保护数据完整性	属于对称体制	运行速度快
1465	多项选择题	GM/T 0009《SM2密码算法使用规范》中，若n为SM2椭圆曲线的阶，则合规的私钥取值包括（ ）。	n	n-1	n-2	n-3
1466	多项选择题	GM/T 0009《SM2密码算法使用规范》中，在SM2密钥协商过程中,发起方计算共享密钥时的输入数据包括（ ）。	自身的公钥	自身的临时公钥	自身的私钥	自身的用户身份标识
1467	多项选择题	GM/T 0009《SM2密码算法使用规范》中，长度为32字节的数据包括（ ）。	SM2签名结果中的R	Z值	默认的用户标识	SM2签名的输入数据
1468	多项选择题	GM/T 0009《SM2密码算法使用规范》中，SM2密文的数据结构中包含有（ ）。	一个随机的椭圆曲线点	一个用于校验的杂凑值	与明文长度相同的密文数据	一个随机数
1469	多项选择题	Shor量子算法容易解决的问题有（ ）。	大整数因子分解问题	离散对数问题	格最小向量问题	NP完全问题
1470	多项选择题	GM/T 0010《SM2密码算法加密签名消息语法规范》中规范了使用SM2密码算法时相关的（ ）。	加密和签名消息语法	加密和签名操作结果的标准化封装	对象标识符	椭圆曲线参数语法
1471	判断题	GM/T 0010《SM2密码算法加密签名消息语法规范》中的数字信封envelopedData数据类型由加密数据和至少一个接收者的数据加密密钥的密文组成。	正确	错误		
1472	判断题	如果采用相同长度的密钥，则椭圆曲线密码的安全性比RSA密码的安全性要高。	正确	错误		
1473	判断题	盲签名比普通的数字签名的安全性要高。	正确	错误		
1474	判断题	如果已知RSA密码体制中的私钥d，则利用公钥可以分解模数n。	正确	错误		

1475	判断题	椭圆曲线密码体制的安全性是基于椭圆曲线离散对数问题的困难性。	正确	错误		
1476	单项选择题	RSA密码体制的安全性，取决于（ ）。	大整数分解	算法的保密性	指数运算	模幂运算
1477	单项选择题	SM2算法的安全级别是（ ）。	256比特	192比特	128比特	512比特
1478	单项选择题	以下不是SM2的应用场景的有（ ）。	生成随机数	协商密钥	加密数据	数据源认证
1479	单项选择题	GM/T 0034《基于SM2密码算法的证书认证系统密码及其相关安全技术规范》中，关于CA管理和操作人员的叙述不正确的是（ ）。	超级管理员负责CA系统的策略设置	业务管理员负责CA系统的某个子系统的业务管理	审计管理员负责对涉及系统安全的事件和各类管理和操作人员的行为进行审计和监督	业务操作员按其权限进行具体的业务操作
1480	单项选择题	GM/T 0034《基于SM2密码算法的证书认证系统密码及其相关安全技术规范》中，关于密钥安全基本要求的叙述不正确的是（ ）。	存在于硬件密码设备之外的所有密钥应加密	对密码设备操作应由多个业务管理员实施	密钥应有安全可靠的备份恢复机制	密钥的生成和使用应在硬件密码设备中完成
1481	单项选择题	GM/T 0034《基于SM2密码算法的证书认证系统密码及其相关安全技术规范》中，CA和KMC的根密钥需要用密钥分割或秘密共享机制分割，（ ）不能成为分管者。	业务操作员	业务管理员	系统维护人员	以上都是
1482	单项选择题	GM/T 0034《基于SM2密码算法的证书认证系统密码及其相关安全技术规范》中，关于密钥库以下说法不正确的是（ ）。	密钥库中的密钥数据应加密存放	分为备用库、在用库和历史库	CA申请的密钥从在用库中取出	历史库存放过期或已被注销的密钥对
1483	单项选择题	GM/T 0034《基于SM2密码算法的证书认证系统密码及其相关安全技术规范》，以下说法不正确的是（ ）。	改变系统的配置如无上级主管批准，操作时应有双人在场	系统出现故障时，应由系统管理人员检查处理，其它人员未经批准不得处理	对CA系统的每次操作都应记录	未经批准不得在服务器上安装任何软件
1484	多项选择题	下列属于公钥的分配方法（ ）。	公用目录表	公钥管理机构	公钥证书	秘密传输

1485	多项选择题	公钥密码体制的基本思想包括（ ）。	将传统分组密码的密钥一分为二，分为加密密钥和解密密钥	加密密钥公开，解密密钥保密	由加密密钥推出解密密钥，在计算上是不可行的	以上都不对
1486	多项选择题	在GM/T 0003.1《SM2椭圆曲线公钥密码算法》中，包含（ ）等部分。	公钥加密	数字签名	密钥交换	身份认证
1487	多项选择题	与SM2算法基于类似数学困难问题的算法包括（ ）。	SM9	RSA	ZUC	ECDSA
1488	多项选择题	SM2算法的应用场景包括（ ）。	数据源认证	消息机密性保护	数据完整性认证	抗抵赖
1489	多项选择题	SM2算法数字签名算法的公开参数有（ ）。	基域规模	椭圆曲线基点	无穷远点	随机数种子
1490	多项选择题	SM2算法涉及到的运算有（ ）。	椭圆曲线点乘	散列值计算	椭圆曲线点加	随机数生成
1491	多项选择题	SM2算法的密钥生成算法涉及到的运算有（ ）。	随机数生成	椭圆曲线点乘	素性检测	因子分解
1492	多项选择题	SM2算法选择的安全椭圆曲线需要满足的条件包括（ ）。	抗MOV攻击	抗异常曲线攻击	抗量子计算攻击	抗GHS攻击
1493	多项选择题	与SM2算法不属于同类型的算法包括（ ）。	RSA	NTRU	SM3	ZUC
1494	多项选择题	SM2数字签名算法可以抵抗的攻击有（ ）。	私钥恢复攻击	存在性伪造攻击	量子计算攻击	强不可伪造攻击
1495	多项选择题	SM2数字签名算法涉及到的运算有（ ）。	随机数生成	椭圆曲线点乘	素性检测	杂凑值计算
1496	多项选择题	SM2数字签名算法的验证过程涉及到的运算有（ ）。	随机数生成	素性检测	椭圆曲线点乘	杂凑值计算
1497	多项选择题	GM/T 0034《基于SM2密码算法的证书认证系统密码及其相关安全技术规范》中，证书认证系统在逻辑上可分为（ ）。	核心层	管理层	服务层	公共层
1498	多项选择题	GM/T 0034《基于SM2密码算法的证书认证系统密码及其相关安全技术规范》中，证书认证系统的管理层包括（ ）。	密钥管理中心	证书管理系统	安全管理系统	证书注册管理系统

1499	多项选择题	GM/T 0034《基于SM2密码算法的证书认证系统密码及其相关安全技术规范》中，密钥管理系统的密钥生成模块应具有（ ）功能。	非对称密钥对的生成	对称密钥的生成	随机数的生成	备用库密钥不足时自动补充
1500	多项选择题	GM/T 0034《基于SM2密码算法的证书认证系统密码及其相关安全技术规范》中，证书的管理安全应满足（ ）要求。	证书申请者的身份应通过验证	由RA签发与申请者身份相符的证书	可以通过审计日志对证书事件进行跟踪	对于证书的任何处理都应作日志记录
1501	判断题	在公钥密码体制中，使用接收方的公钥加密的消息只能被接收方的私钥解密，而公钥是可以公开的，因此，密钥离线分发的必要性就不存在了。	正确	错误		
1502	判断题	GM/T 0034《基于SM2密码算法的证书认证系统密码及其相关安全技术规范》中规定，RA的业务管理员应由CA业务管理员管理。	正确	错误		
1503	判断题	GM/T 0034《基于SM2密码算法的证书认证系统密码及其相关安全技术规范》中规定，密钥恢复操作应由密钥管理中心业务操作员和司法取证人员同时在场。	正确	错误		
1504	判断题	GM/T 0034《基于SM2密码算法的证书认证系统密码及其相关安全技术规范》中规定，证书认证中心对数据变化量少的服务器，可每周做一次备份。	正确	错误		
1505	判断题	SM2 椭圆曲线公钥密码算法不需要验证公钥。	正确	错误		
1506	单项选择题	SM2 椭圆曲线公钥密码算法密钥生成过程中的整数d由（ ）生成。	S盒	伪随机数生成器	密钥流	线性函数
1507	单项选择题	SM2 椭圆曲线公钥密码算法的辅助函数包括（ ）。	填充函数	密码杂凑函数	密钥派生函数	随机数发生器
1508	判断题	SM2 椭圆曲线公钥密码算法用户密钥对包含私钥和公钥。	正确	错误		

1509	单项选择题	下面不是公钥密码算法可依据的难解问题的是（ ）。	大整数分解问题（简称IFP）	离散对数问题（简称DLP）	椭圆曲线离散对数问题（简称ECDLP）	置换-代换
1510	单项选择题	数字信封是用来解决（ ）。	公钥分发问题	私钥分发问题	对称密钥分发问题	数据完整性问题
1511	单项选择题	在公钥密码体制中，用于加密运算的密钥为（ ）。	公钥	私钥	公钥或私钥	以上都不对
1512	单项选择题	关于RSA密码算法下列说法不正确的是（ ）。	RSA算法是一种公钥密码算法	RSA算法可用于某种数字签名方案	RSA的安全性主要基于素因子分解的难度	RSA算法是一种对称加密算法
1513	单项选择题	下边对RSA算法的描述，正确的是（ ）。	RSA是对称密钥算法	RSA是非对称密钥算法	RSA的密钥可以完全公开	RSA的密钥完全保密
1514	单项选择题	下列密码体制的安全性是基于离散对数问题的是（ ）。	Rabin密码	RSA密码	McEliece密码	ElGamal密码
1515	判断题	SM2算法的安全性是基于因子分解困难问题。	正确	错误		
1516	判断题	SM2算法的安全性是基于椭圆曲线离散对数问题。	正确	错误		
1517	判断题	SM2算法可以有效抵抗量子计算攻击。	正确	错误		
1518	判断题	SM2数字签名算法已经入选ISO国际标准。	正确	错误		
1519	判断题	SM2加密算法可以用来保护消息机密性。	正确	错误		
1520	判断题	SM2算法与国际ECDSA算法采用了部分类似的数学结构。	正确	错误		
1521	单项选择题	Rabin密码体制的安全性是基于（ ）。	大整数分解问题	欧拉定理	离散对数问题	背包问题
1522	单项选择题	若Alice想向Bob分发一个会话密钥，采用ElGamal公钥加密算法，那么Alice应该选用的密钥是（ ）。	Alice的公钥	Alice的私钥	Bob的公钥	Bob的私钥
1523	单项选择题	公钥加密与分组加密体制的主要区别是（ ）。	加密强度高	密钥管理方便	密钥长度大	使用一个公共密钥用来对数据进行加密，而一个私有密钥用来对数据进行解密

1524	多项选择题	RSA密码体制中用到了（ ）等数论知识。	Euclidean算法	中国剩余定理	费马小定理	欧拉函数
1525	判断题	SM2算法是对称加密算法。	正确	错误		
1526	判断题	非对称密码体制也称公钥密码体制，即所有的密钥都是公开的。	正确	错误		
1527	判断题	椭圆曲线密码体制的安全性是基于椭圆曲线离散对数问题的困难性。	正确	错误		
1528	判断题	SM2密码算法可用于生成随机数。	正确	错误		
1529	判断题	DSA算法的安全性依赖于求解离散对数问题的难度。	正确	错误		
1530	判断题	若A想向B分发一个会话密钥，采用公钥加密算法，那么A应该选用的加密会话密钥的密钥是A的私钥。	正确	错误		
1531	判断题	RSA公钥密码体制是一种概率密码体制。	正确	错误		
1532	判断题	ElGamal公钥密码体制是一种概率密码体制。	正确	错误		
1533	判断题	我国商用密码SM2签名算法是一种非确定性算法。	正确	错误		
1534	判断题	与RSA算法相比，AES 算法能实现数字签名和数字认证。	正确	错误		
1535	判断题	公钥密码算法中用一个密钥进行加密，而用另一个不相同但是有关的密钥进行解密。	正确	错误		
1536	多项选择题	SM2算法是最为流行的加密算法之一，SM2算法属于加密技术中的（ ）。	对称加密	非对称加密	不可逆加密	以上都是
1537	判断题	RSA算法的安全理论基础是大整数因子分解难题。	正确	错误		
1538	判断题	与RSA算法相比，DES算法能实现数字签名和数字认证。	正确	错误		
1539	判断题	在相同的安全强度条件下，RSA算法所需的密钥长度比椭圆曲线密码算法大。	正确	错误		

1540	单项选择题	在数字签名方案中有签名者和签名验证者，有公钥也有私钥，在验证签名时使用（）。	签名者的公钥	签名者的私钥	验证者的公钥	验证者的私钥
1541	单项选择题	在数字签名方案中有签名者和签名验证者，有公钥也有私钥，在签名时使用（）。	签名者的公钥	签名者的私钥	验证者的公钥	验证者的私钥
1542	单项选择题	可用于实现身份鉴别的安全机制是（ ）。	加密机制和数字签名机制	加密机制和访问控制机制	数字签名机制和路由控制机制	访问控制机制和路由控制机制
1543	多项选择题	Kerberos协议模型中能安装在网络上的实体是（）。	客户机	服务器	网卡	声卡
1544	多项选择题	Kerberos协议使用的凭证有（ ）。	口令	证书	票据	鉴别码
1545	多项选择题	GB/T 15843《信息技术安全技术实体鉴别》，下列说法正确的是（ ）。	给出了采用对称加密算法、数字签名技术和密码校验函数实现机制	采用时间戳、序号或随机数等时变参数防止重放攻击	当采用使用随机数的挑战响应方法时，相互鉴别需要四次传递	生成方在反馈验证方B的权标（TokenAB）中，可通过单向密钥取代可区分标识符
1546	多项选择题	按照GM/T 0022《IPSec VPN技术规范》，以下哪些报文的出现意味着SSL协议正在进行双向身份鉴别（）。	Certificate Request	Client Certificate	Certificate Verify	Client Key Exchange
1547	单项选择题	在量子身份认证方面，以色列密码学者E、Biham等人于（ ）年首先提出了量子身份认证协议，该协议可用于具有对称密钥的通信者之间的身份认证问题。	1996年	1998年	2000年	2001年
1548	多项选择题	在GM/T 0019《通用密码服务接口规范》中，可用于信息机密性保护的函数有（ ）。	计算会话密钥	单块加密运算	结束解密运算	多组数据消息鉴别码运算
1549	判断题	基于口令（PASSWORD）的密钥派生函数需要调用密码杂凑函数。	正确	错误		

1550	判断题	SM9标识密码算法密钥交换过程中不需要计算群中的元素。	正确	错误		
1551	单项选择题	下面容易受到“中间人”攻击的协议是（ ）。	Kerboros密钥传输协议	Diffle－Hellman密钥交换协议	Shamir方案	Guillou-Quisquater识别协议
1552	单项选择题	数字信封通常是用来解决（ ）问题。	公钥分发问题	私钥分发问题	对称密钥分发问题	私钥保密问题
1553	多项选择题	以下可以进行密钥交换的做法是（ ）。	依靠非对称加密算法	依靠专门的密钥交换算法	依靠通讯双方事先已经共享的“秘密”	依靠哈希函数
1554	多项选择题	由于传统的密码体制只有一个密钥，加密密钥等于解密密钥，所以密钥分配过程中必须保证（ ）。	机密性	可用性	真实性	完整性
1555	多项选择题	在GM/T 0024《SSL VPN技术规范》标准中，选用以下哪些密钥交换算法时，是由客户端单独完成预主密钥产生的（ ）。	ECC	IBC	ECDHE	RSA
1556	多项选择题	下列哪种密钥交换协议提供认证性和前向安全性（ ）。	SM2 密钥交换协议	Diffie-Hellman 密钥交换协议	基于椭圆曲线的 Diffie-Hellman 密钥交换协议（ECDH）	MQV 密钥交换协议
1557	多项选择题	以下关于Diffie-Hellman 密钥交换协议说法正确的是（ ）。	Diffie-Hellman 密钥交换协议能提供建立会话密钥的功能	Diffie-Hellman 密钥交换协议不能抵抗中间人攻击	Diffie-Hellman 密钥交换协议不能提供相互认证的安全保障	Diffie-Hellman 密钥交换协议运算在有限循环群上
1558	判断题	在Diffie-Hellman密钥交换中，双方可以通过交换一些可以公开的信息生成出共享密钥。	正确	错误		
1559	判断题	GM/T 0042-2015《三元对等密码安全协议测试规范》中测试平台需要使用信号采集器等设备主动捕采集测试数据。	正确	错误		
1560	判断题	GM/T 0042-2015《三元对等密码安全协议测试规范》中定义的统一封装格式中带有收发标识字段。	正确	错误		

1561	多项选择题	根据密钥信息的交换方式，密钥分发可以分为（）两类。	人工（离线）密钥分发	自动（在线）密钥分发	固定密钥分发	随机密钥分发
1562	单项选择题	SM9密钥交换协议中通信双方共需（ ）次消息传递。	2	3	4	2或3
1563	单项选择题	关于SM9密钥交换协议以下说法错误的是（ ）。	通信双方通过2次信息传递可以协商共享密钥	提供可选的密钥确认功能	基于椭圆曲线双线性对	通过双方主密钥实现密钥协商
1564	单项选择题	以下（ ）算法可以提供密钥交换功能。	SM1	SM3	SM4	SM9
1565	单项选择题	IPSec协议是为了弥补（ ）协议簇的安全缺陷，为IP层及其上层协议提供保护而设计的。	HTTP	IP	SNMP	PPP
1566	单项选择题	IPSec协议中，ISAKMP的全称是（ ）。	AH鉴别头协议	ESP封装安全载荷协议	Internet密钥交换协议	Internet安全关联和密钥管理协议
1567	单项选择题	UDP、TCP和SCTP都是（ ）层协议。	物理	数据链路	网络	传输
1568	单项选择题	SSH1.0是一种不安全的远程管理协议，原因之一即其使用了（ ）来保证数据的完整性。	HMAC	CMAC	CRC	NMAC
1569	单项选择题	下列不是SSL所提供的服务是（ ）。	用户和服务器的身份鉴别	数据加密传输	数据完整性保护	通信双方通信时的基本信息
1570	单项选择题	针对多数据源模型训练的隐私保护可以利用（ ）技术，主要用于多个移动终端用户协同训练一个模型。	安全多方计算	联邦学习	可信执行环境	区块链
1571	多项选择题	SSL协议可以实现的安全需求有（ ）。	服务器对用户身份认证	用户对服务器身份认证	传输信息的机密性	传输信息的完整性
1572	多项选择题	SSL协议体系结构包括的协议子层是（ ）。	握手协议层	记录协议层	发送数据层	接收数据层
1573	多项选择题	SSL协议提供的安全通道具有的特征有（ ）。	机密性	真实性	完整性	高效、快速
1574	单项选择题	IPSec协议不可以做到（ ）。	通信实体认证	完整性检查	加密	签发证书

1575	单项选择题	基于（ ）加密的密文检索方法可以直接对加密数据进行检索，有效降低运算复杂度的同时不改变相应的明文顺序，既保护了用户数据安全，又提高了密文检索效率。	秘密共享	全同态	区块链	不经意传输
1576	单项选择题	IPSec协议中的SA分为IPSec SA和IKE SA，其中单个IPSec SA是（ ），单个IKE SA是（ ）。	单向，双向	单向，单向	双向，双向	双向，单向
1577	单项选择题	SSL协议中，记录层协议将数据分为长度为（ ）或更小的数据块。	1KB	4KB	16KB	64KB
1578	单项选择题	下面哪个说法在SSL握手协议中的过程是错误的（ ）。	预主密钥生成主密钥	主密钥生成工作密钥	hello消息中协商密码套件	主密钥生成预主密钥
1579	单项选择题	当ESP处于（ ）情况下，ESP头放在新建外部IP头之后，原IP数据报文之前，为整个原IP报文提供机密性保护，为新建外部IP头后的内容提供认证保护。	主模式	快速模式	传输模式	隧道模式
1580	单项选择题	SSL协议采用两套密钥分别用于两个方向的通信，IPSec使用两个单向的IPSec SA实现双向通信，这样设计可以防范（ ）。	重放攻击	中间相遇攻击	中间人攻击	侧信道攻击
1581	多项选择题	参照GM/T 0024标准实现的SSL协议，以下说法正确的是（ ）。	Hello消息中，双方交换的随机数用于派生出主密钥	对服务端进行身份鉴别时采用数字签名方式，若密钥交换方式为ECDHE，则签名数据中包含有服务端密钥交换参数	IBC_SM4_SM3密码套件中采用SM9算法实现身份鉴别	生成密钥的PRF算法可用SM3实现
1582	多项选择题	参照GM/T 0022标准实现的IPSec协议，以下说法错误的是（ ）。	用于通信隧道传输保护的会话密钥是在IKE阶段快速模式中生成的	ESP封装模式下，可对整个IP报文提供加密保护	传输模式下，AH子协议对原有IP报文和新加IP头提供完整性、数据源鉴别安全功能	IKE阶段主模式中，密钥协商时的密钥素材是直接采用对方加密公钥实现机密性传输保护的

1583	多项选择题	以下关于SSL/TLS说法，正确的是（ ）。	使用SSL/TLS可以确保通信报文的机密性	在SSL/TLS中，使用数字签名技术来认证通信双方的身份	在SSL/TLS中，可以确保通信报文的完整性	在SSL/TLS中，一定是实现了双向身份鉴别
1584	多项选择题	参照GM/T 0024标准实现的SSL协议，握手协议的描述错误的是（ ）。	在客户端和服务端Hello消息之后，服务端向客户端发送服务端证书且必须向客户端发送证书请求消息	在对交换数据进行加密和签名计算时，交换数据的加密和签名运算可以采用同一公私钥对	客户端和服务端之间使用的密钥交换算法由协议的版本决定	工作密钥的具体密钥长度由选用的密码算法决定
1585	判断题	在测评时，发现在SSL协议的Client Hello报文中出现了{0xe0,0x13}属性值，那么意味着该链路正在使用ECC_SM4_SM3套件。	正确	错误		
1586	判断题	经抓包发现通信双方协商的密码套件为ECDH_RSA_WITH_AES_256_CBC_SHA和ECDHE_RSA_WITH_AES_256_CBC_SHA，前者无法提供前向安全性，而后者可以提供。	正确	错误		
1587	判断题	经抓包发现通信双方协商的密码套件为ECC_SM4_SM3和ECDHE_SM4_SM3，前者无法提供前向安全性，而后者可以提供。	正确	错误		
1588	判断题	经抓包发现通信双方协商的密码套件为RSA_WITH_AES_256_CBC_SHA，该套件无法提供前向安全性。	正确	错误		
1589	判断题	通过协议解析工具可以解析ISAKMP协议第二阶段（快速模式）中除了协议头之外的数据包。	正确	错误		

1590	判断题	TLS 1.0 版本协议中CBC模式的IV没有使用不可预测的随机数，而是使用了上一次 CBC 模式加密时的最后一个分组，从而导致被攻击。因此，为了防御此类攻击，TLS 1.1以上的版本中要求必须隐式地传送IV。	正确	错误		
1591	判断题	SSL协议中，最终客户端和服务端会生成一对密钥，用于双方通信时对数据报文加密和校验。	正确	错误		
1592	判断题	在TLS1.2协议中，如果客户端和服务端选用密码套件ECDHE-RSA-AES256-CBC-SHA256，那么SHA256的作用是用于数据报文的完整性保护。	正确	错误		
1593	判断题	仅使用HTTPS就可以保障网上支付各个环节的安全性。	正确	错误		
1594	单项选择题	SSL协议的密码套件中，经抓包发现通信双方协商的密码套件为ECDHE_RSA_WITH_AES_128_GCM_SHA，下列说法错误的是（ ）。	RSA算法用于实现身份鉴别	基于RSA数字信封方式进行密钥交换	AES-GCM算法用于实现通信数据机密性保护	AES-GCM算法用于实现通信数据完整性保护
1595	单项选择题	以下最适合用于支持NAT（网络地址转换）穿越的模式是（ ）。	传输模式下使用AH+ESP协议	隧道模式下使用AH+ESP协议	传输模式下使用ESP协议	隧道模式下使用ESP协议
1596	判断题	SSL/TLS可以确保通信的机密性，还可以防止数据被篡改，但无法对服务器进行认证。	正确	错误		
1597	单项选择题	S-HTTP（安全超文本传输协议）是一种结合HTTP 而设计的安全通信协议，它工作（ ）层。	传输层	链路层	网络层	应用层
1598	单项选择题	在IPSec中，设计AH协议的主要目的是用来增加IP数据包（ ）的认证机制。	安全性	完整性	可靠性	机密性
1599	多项选择题	SSL记录协议（Record Protocol）为SSL连接提供的服务有（ ）。	保密性	便捷性	高效性	完整性

1600	判断题	在实际应用中，一般使用主密钥对通信数据进行加密。	正确	错误		
1601	单项选择题	GM/T 0005《随机性检测规范》中规定的显著性水平是（ ）。	0.1	0.01	0.001	0.0001
1602	单项选择题	GM/T 0005《随机性检测规范》中，“线性复杂度检测”中计算线性复杂度，通常采用以下哪种算法（ ）。	Miller-Rabin算法	Berlekamp-Massey算法	最小二乘法	中国剩余定理
1603	单项选择题	在随机数发生器后处理方法中，并非冯·诺依曼后处理方法特点的是（ ）。	输入序列是统计独立的	输出速率是稳定的	输入序列会被压缩输出	输入序列是不均衡的
1604	多项选择题	GM/T 0005《随机性检测规范》中，关于检测原理以下说法正确的是（ ）。	“Maurer通用统计检测”用于检测待检序列能否被无损压缩，如果待检序列能被显著地压缩，那么就认为该序列是不随机的	“重叠子序列检测”通过比较m位可重叠子序列模式的频数和m+1位可重叠子序列模式的频数来检测其随机性	“扑克检测”用于检测待检序列中m位非重叠子序列的每一种模式的个数是否接近	“矩阵秩检测”用于检测待检序列中给定长度的子序列之间的线性独立性
1605	多项选择题	根据GM/T 0005《随机性检测规范》，若指定样本数量是1000，以下通过测试的组是（ ）。	通过样本数量是970	通过样本数量是975	通过样本数量是981	通过样本数量是985
1606	多项选择题	以下会用到随机数的场景有（ ）。	生成初始化向量（IV）	生成对称密钥	生成密钥对	生成nonce
1607	判断题	GM/T 0005《随机性检测规范》中，“块内频数检测”用于检测待检序列中0和1的个数是否相近。	正确	错误		
1608	判断题	GM/T 0005《随机性检测规范》中，“离散傅立叶检测”用于检测待检序列进行傅立叶变换后得到不正常的峰值个数是否超过了允许值。	正确	错误		
1609	判断题	对称加密算法和密码杂凑算法具有混淆和扩散的特性，数据经过其处理后，将呈现非常良好的随机特性，因此很多时候，它们可以单独使用以产生真随机数。	正确	错误		

1610	判断题	伪随机数生成器产生的序列不一定具备不可预测性。	正确	错误		
1611	判断题	随机数一定是不可预测的，所以由随机数发生器产生的随机数不会出现连续多个'0'的情况。	正确	错误		
1612	判断题	SM2签名算法用到的随机数不可泄露，但可以重复使用。	正确	错误		
1613	判断题	随机数发生器输出的必须是熵源产生的直接结果，不能经过后处理。	正确	错误		
1614	判断题	软件密码模块（或混合密码模块的软件部件）中的随机数发生器部件，可以单独作为软件密码模块，也可以作为软件密码模块（或混合密码模块的软件部分）的一部分。	正确	错误		
1615	单项选择题	下列需要由双方或多方共同提供信息建立起共享会话密钥的协议是（ ）。	密钥建立协议	密钥传输协议	密钥共享协议	密钥协商协议
1616	单项选择题	以下密钥建立方式，如果长期密钥泄露，将会导致之前协商的会话密钥也被泄露的是（ ）。	DH协议	MQV协议	ECDH协议	数字信封技术
1617	单项选择题	如果有6个成员组成的团体希望互相通信，那么在点到点的对称密钥分发结构中，需要人工分发密钥加密密钥（KEK）的数量为（ ）。	18	3	15	18
1618	单项选择题	如果有6个成员组成的团体希望互相通信，那么在在基于密钥中心的对称密钥分发结构中，需要人工分发KEK的数量为（ ）。	5	8	6	15
1619	多项选择题	在密钥分发场景中，常见做法有（ ）。	人工传递	知识拆分	通过密钥加密密钥（KEK）加密传输	数字信封
1620	多项选择题	以下哪些密码系统的参数应该与密钥一样进行保护（ ）。	SM4加密过程中的轮密钥	密码算法中随机数发生器的内部状态	椭圆曲线密码体制所使用的域的参数	SM2密钥交换临时产生的随机数
1621	判断题	RC4是一个典型的基于非线性数组变换的序列密码。为了保证安全的强度，要求至少使用64位密钥，以防止穷举搜索攻击。	正确	错误		

1622	判断题	签名私钥和加密私钥都应及时进行归档。	正确	错误		
1623	判断题	密钥分散是上级的密钥与本级的特征相结合形成本级的密钥，其基本思想是用密钥来保护密钥。	正确	错误		
1624	多项选择题	有中心的密钥分发模式中，会话密钥可以由（ ）生成。	通信发起方	认证服务器	代理服务器	密钥分发中心KDC
1625	判断题	以点对点密钥分发协议为例，在一个有n个用户的系统中，需要保存n(n-1)个密钥。	正确	错误		
1626	单项选择题	假设某公司的董事会想保护产品的配方，该公司总裁应该能够在需要时拿到配方，但在紧急的情况下，12位董事会成员中的任意7位也可以揭开配方。在密码学上，解决这类问题的技术称为（ ）。	密钥托管技术	门限密钥协商技术	密钥分发技术	门限秘密共享技术
1627	单项选择题	密钥管理负责从初始产生到最终销毁的整个过程，通常包括密钥的生成、（ ）、分发、使用、备份与恢复、更新、撤销和销毁等内容。	交换	存储	延续	删除
1628	多项选择题	通过密钥生成器生成的密钥要确保它的（ ）。	可重复性	不可重复性	不可预测性	抗抵赖性
1629	多项选择题	下面关于密钥管理的说法正确的是（ ）。	非对称密钥中的公钥不需要机密性保护，但应该考虑完整性保护	密钥分发包括人工方式和在线方式	密钥管理技术可包括：对称密钥管理和非对称密钥管理	密钥安全性应综合密钥空间、密钥使用时长等因素
1630	多项选择题	以下关于密钥派生的说法正确的有（ ）。	从口令派生密钥可用于加密存储设备	从口令派生密钥可用于网络通信数据保护	可以基于HMAC算法实现	可以基于CMAC算法实现
1631	判断题	密钥管理就是在授权各方之间实现密钥关系的建立和维护的一整套技术和程序，只要密钥管理策略是安全的，那么就不会发生密钥泄露等问题。	正确	错误		

1632	判断题	现代密码体制要求密码算法是可以公开评估的，整个密码系统的安全性并不取决对密码算法的保密或者是对密码设备等保护，决定整个密码体制安全性的因素是密钥的保密性。	正确	错误		
1633	判断题	密钥管理遵循“木桶”原理，即密钥的安全性是由密钥整个阶段中安全性最低的阶段决定的。	正确	错误		
1634	判断题	信息系统中的密钥在其生命周期内涉及到生成、存储、导入和导出、分发、使用、备份和恢复、公开、销毁等环节。	正确	错误		
1635	判断题	并非所有的密钥都需要存储，一些临时密钥或一次一密的密钥在使用完就要进行销毁。	正确	错误		
1636	判断题	任何密钥的使用都应遵循密钥的生存周期,绝不能超期使用,这是因为密钥使用时间越长,重复几率越大，外泄可能性越大，被破译的危险性就越大。	正确	错误		
1637	判断题	会话密钥可由通信双方协商得到，也可由密钥分发中心分配。	正确	错误		
1638	判断题	按照是否需要第三方可信机构来分,秘密密钥分发分为无中心的密钥分发和有中心的密钥分发两种方式。	正确	错误		
1639	判断题	密钥协商的目的是通信双方在网络中通过交换信息生成一个双方共享的会话密钥。	正确	错误		
1640	判断题	密钥管理最小权利策略是指分配给用户进行某一事物处理所需的最小的密钥集合。	正确	错误		
1641	判断题	在密码算法强度足够大的情况下，密钥可以不用更新。	正确	错误		
1642	多项选择题	GM/Z 4001《密码术语》中，密钥全生命周期包括（ ）等。	密钥产生	密钥存储	密钥更新	密钥分量
1643	多项选择题	数字签名使用密码杂凑函数预先处理消息，可以（ ）。	防范伪造攻击	提高签名的计算速度	缩小待签名消息的长度	提高签名验证的速度

1644	单项选择题	签名者无法知道所签消息的具体内容，即使后来签名者见到这个签名时，也不能确定当时签名的行为，这种签名称为（ ）。	代理签名	群签名	多重签名	盲签名
1645	单项选择题	一个数字签名体制包含的内容，说法正确的是（ ）。	包含加密和解密两个方面	包含加密和认证两个方面	包含签名和验证签名两个方面	包含认证和身份识别两个方面
1646	单项选择题	关于数字签名，以下说法正确的是（ ）。	数字签名是在所传输的数据后附加上一段和传输数据毫无关系的数字信息	数字签名能够解决数据的加密传输，即安全传输问题	数字签名一般采用对称加密机制	数字签名能够解决篡改、伪造等安全性问题
1647	单项选择题	下面对于数字签名的描述不正确的是（ ）。	数字签名是可信的	数字签名是不可抵赖的	数字签名是可伪造的	数字签名是不可伪造的
1648	单项选择题	下面的说法中错误的是（ ）。	对称密码系统的加密密钥和解密密钥相同	PKI系统的加密密钥和解密密钥不同	数字签名之前要先对消息或报文做摘要	数字签名系统一定具有数据加密功能
1649	单项选择题	下面有关盲签名说法错误的是（ ）。	消息的内容对签名者是不可见的	在签名被公开后，签名消息一定可追踪	消息的盲化处理由消息拥有者完成	满足不可否认性
1650	单项选择题	下面有关群签名说法错误的是（ ）。	只有群成员能代表这个群组对消息签名	验证者可以确认数字签名来自于该群组	验证者能够确认数字签名是哪个成员所签	借助于可信机构可以识别出签名是哪个签名人所为
1651	单项选择题	与RSA算法相比，DSS（数字签名标准）不包括（ ）。	数字签名	鉴别机制	加密机制	数据完整性
1652	单项选择题	签名者把他的签名权授给某个人，这个人代表原始签名者进行签名，这种签名称为（ ）。	代理签名	群签名	多重签名	盲签名
1653	多项选择题	关于消息认证，以下说法正确的是（ ）。	可以验证消息来源	可以验证消息的完整性	可以验证消息的真实性	可以加密消息
1654	单项选择题	环签名(ring signature)是一种（ ）方案，是一种简化的群签名,环签名中只有环成员没有管理者,不需要环成员间的合作。	加密	数字签名	数字认证	秘密共享
1655	多项选择题	可以构造环签名的我国标准算法是（ ）。	SM2	SM3	SM4	SM9

1656	多项选择题	GB/T 17903《信息技术 安全技术 抗抵赖》提供的抗抵赖机制可用于如下阶段的抗抵赖（ ）。	证据生成	证据传输、存储和检	证据验证	争议仲裁
1657	单项选择题	关于SM9数字签名算法以下说法错误的是（ ）。	基于椭圆曲线双线性对实现	签名之前需要对待签消息进行压缩	使用主私钥对待签消息进行签名	可通过签名者标识和其他信息对签名进行验证
1658	单项选择题	签名者无法知道所签消息的具体内容，即使后来签名者见到这个签名时，也不能确定当时签名的行为，这种签名称为（ ）。	代理签名	群签名	多重签名	盲签名
1659	单项选择题	下列方法通常用来实现抗抵赖性的是（ ）。	加密	数字签名	时间戳	哈希值
1660	单项选择题	下列不属于数字签名所能实现的安全保证的是（ ）。	保密通信	防抵赖	防冒充	防伪造
1661	多项选择题	完整的数字签名过程包括（ ）过程。	加密	解密	签名	验证
1662	多项选择题	现代密码学中很多应用包含散列运算，下面应用中包含散列运算的是（ ）。	消息机密性	消息完整性	消息认证码	数字签名
1663	多项选择题	盲签名与普通签名相比，其显著特点为（ ）。	签名者是用自己的公钥进行签名	签名者不知道所签署的数据内容	签名者先签名，然后再加密自己的签名，从而达到隐藏签名的目的	在签名被接收者泄露后，签名者不能跟踪签名
1664	多项选择题	数字签名应该具有的特征有（ ）。	不可伪造	不可泄露	不可改变	不可否认
1665	多项选择题	下列方法可用于消息认证是（ ）。	消息认证码（MAC）	数字签名	杂凑函数	信息隐藏
1666	判断题	根据仲裁的参与情况可将数字签名分为两种类型：真实签名和仲裁签名。仲裁签名在实现的过程中一直需要仲裁的参与，也就是说在签名算法的实现过程中需要利用仲裁的“可信性”作为算法的一部分。	正确	错误		
1667	判断题	消息认证码（MAC）具有认证功能。	正确	错误		

1668	判断题	群签名中任意群成员可代表整个群组对消息签名。	正确	错误		
1669	多项选择题	下列哪些是公钥基础设施PKI的常见部件（ ）。	CA中心	证书库	证书撤销管理系统	密钥分发中心KDC
1670	多项选择题	以下哪些是数字证书的构成要素（ ）。	证书颁发者	密钥用法	签发时间	私钥
1671	多项选择题	我国双证书体系中包括签名证书和加密证书，依据GM/T0015《基于SM2密码算法的数字证书格式规范》，其中加密证书可用于（ ）。	数据加密	密钥加密	数字签名	密钥协商
1672	多项选择题	下列关于数字证书和公钥基础设施PKI的说法正确的是（ ）。	证书是CA机构将用户的公钥进行加密之后的产物	要确认证书中所包含的公钥是否合法，需要得到CA机构的公钥	世界上颁发的所有证书，沿着CA机构的层级关系都能够找到唯一的根CA	用户发现自己的私钥泄露之后，需要联系CA机构申请证书撤销
1673	单项选择题	PKI体系所使用数字证书的格式标准是（ ）。	RSA	PGP	X.509	ECC
1674	单项选择题	PKI是（ ）的简称。	Private Key Infrastructure	Public Key Infrastructure	Public Key Institute	Private Key Institute
1675	多项选择题	证书的生命周期包括以下哪些（ ）。	证书申请	证书生成	证书存储	证书撤销
1676	多项选择题	从密钥用途上来分，数字证书可以分为（ ）。	加密证书	个人证书	签名证书	公共证书
1677	多项选择题	数字证书的申请方式有（ ）。	在线申请	离线申请	普通申请	贵宾申请
1678	多项选择题	我国PKI的部件主要包括（ ）。	签发证书的证书机构CA	登记证书的注册机构RA	存储和发布证书的电子目录	密钥管理系统KM
1679	单项选择题	下面哪个格式描述了证书请求语法（ ）。	PKCS#7	PKCS#8	PKCS#9	PKCS#10
1680	单项选择题	以下关于GM/T 0034《基于SM2密码算法的证书认证系统密码及其相关安全技术规范》描述错误的是（ ）。	证书申请和下载可以采用在线或离线两种方式	用户签名密钥对和加密密钥对均由用户自己产生	用户的数字证书由CA签发，根CA的数字证书由根CA自己签发，下级CA的数字证书由上级CA签发	证书状态查询系统所提供的服务可以采用CRL查询或在线证书状态查询两种方式

1681	单项选择题	以下哪项不是CA的服务功能（ ）。	提供加密私钥管理	用户证书签发	用户证书撤销	用户证书查询
1682	判断题	X.509签名证书中，signatureAlgorithm域包含了该证书对应私钥签名时所使用的的密码算法标识符。	正确	错误		
1683	单项选择题	公钥密码体制中，其他人可以用公钥进行（ ）。	加密和验证签名	解密	签名	以上均不对
1684	单项选择题	X.509数字证书格式中包含的元素有①证书版本②证书序列号③签名算法标识④证书有效期⑤证书颁发者⑥证书主体名⑦主体公钥信息和⑧（ ）。	主体的解密密钥	证书序列号摘要	密钥交换协议	签名值
1685	单项选择题	数字证书由CA机构签发，用（ ）来验证证书。	私钥	公钥	SRA	序列号
1686	单项选择题	在 PKI 系统中，由（ ）绑定用户的身份信息和公钥。	发送方	CA机构	接收方	不需要
1687	单项选择题	CA用( )签名数字证书。	用户的公钥	用户的私钥	自己的公钥	自己的私钥
1688	多项选择题	数字证书的基本内容包括( )。	用户标识	用户公钥	用户私钥	CA签名
1689	多项选择题	密钥管理包括哪些内容( )。	密钥产生	密钥备份	密钥恢复	密钥更新
1690	多项选择题	以下关于PKI的叙述正确的是（ ）。	PKI是利用公钥理论和技术建立的提供安全服务的基础设施	CA是证书的签发机构，也是PKI的核心	PKI的基础技术包括加密、数字签名、数据完整性机制、数字信封、双重数字签名等	RA主要进行用户的注册和审核
1691	多项选择题	PKI的基本组成包括（ ）。	CA	KM	RA	密钥分发中心
1692	判断题	PKCS#1描述了RSA加密和解密的方法 。	正确	错误		
1693	单项选择题	GM/T 0015《基于SM2密码算法的数字证书格式规范》中，对于双证书，标准的证书扩展域的（ ）一定为关键项。	密钥用法keyUsage	主体密钥标识符subjectKeyIdentifier	扩展密钥用途extKeyUsage	认证机构authority

1694	单项选择题	GM/T 0015《基于SM2密码算法的数字证书格式规范》中，关于证书扩展项说法不正确的是（ ）。	扩展项包括两部分：扩展关键度和扩展项值	采用关键性的扩展项可能导致在通用的应用中无法使用证书	颁发机构密钥标识符authorityKeyIdentifier也可用作CRL扩展	如果不能识别关键的扩展时，应拒绝接受该证书
1695	单项选择题	GM/T 0015《基于SM2密码算法的数字证书格式规范》标准中ASN.1采用了（ ）编码。	DER	OER	PER	XER
1696	判断题	GM/T 0015《基于SM2密码算法的数字证书格式规范》中，CA在2049年之前应将有效期时间编码为UTCTime类型。	正确	错误		
1697	判断题	GM/T 0015《基于SM2密码算法的数字证书格式规范》中，CA应确保使用大于20个8位字节的证书序列号。	正确	错误		
1698	多项选择题	下列选项中是CA证书的组成部分的是（ ）。	证书序列号（唯一的）	证书持有者名称	证书颁发者名称	证书有效期
1699	判断题	公钥证书主要用于确保公钥及其与用户绑定关系的安全。公钥证书的持证主体可以是人、设备、组织机构或其它主体。	正确	错误		
1700	判断题	在GM/Z4001《密码术语》中，公钥基础设施（PKI）可用于提供机密性、完整性、真实性及抗抵赖等安全服务。	正确	错误		
1701	判断题	用户可以通过公钥证书来相互交换自己的公钥，不需要每次都联系CA机构。	正确	错误		
1702	单项选择题	防止他人对传输的文件进行破坏，以及确定发信人的身份需要采取的密码技术手段是（ ）。	数字签名	加密技术	生物识别	实体鉴别
1703	多项选择题	下面属于身份鉴别的主要方法有（ ）。	基于口令	基于硬件Token	基于生物特征	访问控制
1704	多项选择题	多因素鉴别的因子可以包括哪些（ ）。	口令	令牌	指纹	手势

1705	判断题	JWT（Json Web Token）常用于各类身份鉴别与授权应用场景中，仅支持对称密码算法实现Token的生成。	正确	错误		
1706	单项选择题	下面有关数字签名描述错误的是（ ）。	通过待签名消息、签名值和公钥完成签名验证	发送者事后不能抵赖对报文的签名	接收者不能伪造签名	能够保证待签名消息的机密性
1707	多项选择题	对用户的身份鉴别基本方法可以分为（ ）。	基于虹膜的身份鉴别	基于秘密信息的身份鉴别	基于指纹的身份鉴别	基于人脸的身份鉴别
1708	多项选择题	身份鉴别是指确认一个人的身份信息。身份鉴别可通过（ ）实现。	用户知道什么	用户的指纹特征	用户拥有什么	用户的虹膜特征
1709	判断题	数字证书采用公钥密码体制，每个用户都可以设定公钥，其公钥用于用于解密和签名。	正确	错误		
1710	判断题	数字证书中一般由证书拥有者对其公钥进行签名。	正确	错误		
1711	多项选择题	身份认证的作用是对用户的身份进行鉴别，能保护网络信息系统中的数据和服务不被未授权的用户访问。身份认证技术包括（ ）。	用户名+口令	动态令牌	生物特征认证	数字签名技术
1712	单项选择题	智能密码钥匙中用于签名和签名验证的密钥是（）。	设备认证密钥	用户密钥	会话密钥	对称密钥
1713	多项选择题	在GM/T 0027《智能密码钥匙技术规范》中规定了智能密码钥匙的功能要求、硬件要求等，还规定了哪些要求（）。	软件要求	性能要求	环境适应性要求	可靠性要求
1714	多项选择题	在GM/T 0027《智能密码钥匙技术规范》中，功能要求中的初始化要求包括（）。	出厂初始化	设备初始化	应用初始化	个人化数据初始化
1715	多项选择题	在GM/T 0027《智能密码钥匙技术规范》的密码运算功能要求中，分组密码算法的工作模式至少应包括哪些（）。	电子密码本（ECB）	密码分组链接（CBC）	输出反馈（OFB）	密文反馈（CFB）
1716	多项选择题	根据GM/T 0027《智能密码钥匙技术规范》，智能密码钥匙必须至少支持三种密钥，分别是（）。	设备认证密钥	用户密钥	会话密钥	密钥加密密钥

1717	多项选择题	根据GM/T 0027《智能密码钥匙技术规范》，智能密码钥匙的硬件要求包括哪些方面（）。	接口	芯片	线路传输	密钥安全
1718	多项选择题	根据GM/T 0027《智能密码钥匙技术规范》，在管理终端和智能密码钥匙之间传输的所有口令和密钥有什么要求（）。	均应加密传输	传输过程中能够防范重放攻击	可以明文传输	必须保证不可否认性
1719	多项选择题	根据GM/T 0027《智能密码钥匙技术规范》，智能密码钥匙要能够具备抵抗的攻击包括（）。	能量分析攻击	电磁分析攻击	时间分析攻击	错误注入攻击
1720	多项选择题	根据GM/T 0027《智能密码钥匙技术规范》，智能密码钥匙在哪些功能需要支持掉电保护（）。	密钥生成	密码运算	文件读写	口令验证和修改
1721	多项选择题	根据GM/T 0027《智能密码钥匙技术规范》，智能密码钥匙的安全要求包括设备软件安全防护等，还有哪些部分的安全要求（）。	密码算法	密钥管理	多应用安全	线路传输安全
1722	判断题	根据GM/T 0027《智能密码钥匙技术规范》，智能密码钥匙的硬件接口只能是USB接口。	正确	错误		
1723	判断题	根据GM/T 0027《智能密码钥匙技术规范》，智能密码钥匙在设备发行时，必须对设备认证密钥进行修改。	正确	错误		
1724	判断题	根据GM/T 0027《智能密码钥匙技术规范》，智能密码钥匙的所有私钥都应在密码钥匙内部生成。	正确	错误		
1725	判断题	根据GM/T 0027《智能密码钥匙技术规范》，智能密码钥匙的加密私钥既可以导入也可以导出。	正确	错误		
1726	单项选择题	根据GM/T 0027《智能密码钥匙技术规范》，下列算法中，不是智能密码钥匙必须支持的是（）	公钥密码算法	流密码算法	分组密码算法	杂凑算法
1727	单项选择题	根据GM/T 0027《智能密码钥匙技术规范》，下列哪个不是智能密码钥匙应用初始化阶段进行的操作（）	设置管理员口令	设置用户口令	对设备认证密钥进行初始化	设置应用中容器个数

1728	单项选择题	根据GM/T 0027《智能密码钥匙技术规范》，智能密码钥匙必须支持的公钥密码算法是（）	RSA1024	RSA2048	SM2	SM3
1729	单项选择题	根据GM/T 0027《智能密码钥匙技术规范》，以下哪个不是智能密码钥匙必须支持的密钥类型（）	设备认证密钥	用户密钥	会话密钥	AES密钥
1730	判断题	根据GM/T 0027《智能密码钥匙技术规范》，在管理终端和智能密码钥匙之间传输的所有口令和密钥均应加密传输，并保证在传输过程中能够防范重放攻击。	正确	错误		
1731	单项选择题	根据GM/T 0016《智能密码钥匙密码应用接口规范》，容器中存放的加密密钥用于保护哪种密钥（）。	解密私钥	验签公钥	加密公钥	会话密钥
1732	单项选择题	根据GM/T 0016《智能密码钥匙密码应用接口规范》，设备出厂阶段，应执行哪种操作（）。	预置SM2签名预处理信息	预置加密密钥对	预置会话密钥	预置设备认证密钥
1733	单项选择题	根据GM/T 0016《智能密码钥匙密码应用接口规范》，PIN码长度至少为几个字节（）。	4	6	8	10
1734	单项选择题	根据GM/T 0016《智能密码钥匙密码应用接口规范》，以下哪种密钥可以以明文形式出现在设备之外（）。	解密私钥	加密公钥	签名私钥	会话密钥
1735	单项选择题	根据GM/T 0016《智能密码钥匙密码应用接口规范》，应用管理不包含以下哪个接口函数（）。	应用枚举	应用删除	应用关闭	取得创建应用的权限
1736	单项选择题	在GM/T 0016《智能密码钥匙密码应用接口规范》中，以下陈述正确的是（）。	容器可以包含多个应用	应用可以包含多个容器	容器可以包含多个文件	应用之间可以互相依赖
1737	单项选择题	在GM/T 0016《智能密码钥匙密码应用接口规范》中，以下陈述正确的是（）。	智能密码钥匙中的应用之间应相互独立	智能密码钥匙可拥有多个设备认证密钥	容器中应包含设备认证密钥	应用中应包含设备认证密钥
1738	多项选择题	在GM/T 0016《智能密码钥匙密码应用接口规范》中，应用由以下哪些组件构成（）。	管理员PIN	用户PIN	文件	容器

1739	多项选择题	在GM/T 0016《智能密码钥匙密码应用接口规范》中，容器中存放了哪些敏感信息（）。	加密密钥对	签名密钥对	会话密钥	随机数发生器状态
1740	多项选择题	在GM/T 0016《智能密码钥匙密码应用接口规范》中，文件管理函数包括如下哪些功能（）。	创建文件	删除文件	枚举文件	获取文件信息
1741	多项选择题	在GM/T 0016《智能密码钥匙密码应用接口规范》中，计算多组数据消息鉴别码的操作包括（）。	SKF_MacInit	SKF_MacUpdate	SKF_MacFinal	SKF_DigestFinal
1742	多项选择题	在GM/T 0016《智能密码钥匙密码应用接口规范》中，个人身份识别码包括哪些类型（）。	管理员PIN	用户PIN	设备验证密钥	报文鉴别码MAC
1743	多项选择题	在GM/T 0016《智能密码钥匙密码应用接口规范》中，规定的权限包括哪些（）。	设备权限	用户权限	管理员权限	日志权限
1744	多项选择题	根据GM/T 0016《智能密码钥匙密码应用接口规范》，正确的陈述包括哪些（）。	管理员PIN码验证通过后，获得管理员权限，管理员权限只作用于其所在的应用	用户PIN码验证通过后，获得用户权限，用户权限只作用于其所在的应用	通过设备认证后获得设备权限	一个应用中可以包含多个容器
1745	判断题	根据GM/T 0016《智能密码钥匙密码应用接口规范》，一个设备中存在唯一一个设备认证密钥和唯一一个应用	正确	错误		
1746	判断题	根据GM/T 0016《智能密码钥匙密码应用接口规范》，加密密钥对由外部产生并安全导入。	正确	错误		
1747	判断题	根据GM/T 0016《智能密码钥匙密码应用接口规范》，会话密钥可以由外部产生并安全导入。	正确	错误		
1748	判断题	根据GM/T 0016《智能密码钥匙密码应用接口规范》，签名密钥对应由内部产生，而加密密钥对应由外部产生并安全导入。	正确	错误		

1749	判断题	根据GM/T 0016《智能密码钥匙密码应用接口规范》，其支持的接口函数类型包括设备管理、访问控制、应用管理、文件管理、容器管理和密码服务。	正确	错误		
1750	判断题	根据GM/T 0016《智能密码钥匙密码应用接口规范》，加密密钥对保护结构中对称算法标识所确定的加密模式为ECB模式。	正确	错误		
1751	判断题	根据GM/T 0016《智能密码钥匙密码应用接口规范》，支持的设备权限类型包括管理员权限和用户权限。	正确	错误		
1752	判断题	在GM/T 0016《智能密码钥匙密码应用接口规范》中定义了智能密码钥匙的开发接口。	正确	错误		
1753	判断题	根据GM/T 0016《智能密码钥匙密码应用接口规范》，设备密钥用于应用程序对智能密码钥匙身份的认证。	正确	错误		
1754	单项选择题	根据GM/T 0016《智能密码钥匙密码应用接口规范》，验证管理员PIN成功后，可以进行哪些操作（）。	删除应用文件	删除会话密钥	修改用户PIN	修改管理员PIN
1755	单项选择题	根据GM/T 0016《智能密码钥匙密码应用接口规范》，验证用户PIN成功后，可以进行以下操作（）	修改设备密钥	修改管理员PIN	修改用户PIN	初始化设备
1756	单项选择题	在GM/T 0016《智能密码钥匙密码应用接口规范》中，关于权限使用说法正确的是（）	设备权限仅用于创建应用、删除应用和修改设备认证密钥	创建和删除容器需要管理员权限	文件的读写权限在使用文件时指定	容器内私钥的使用需要管理员权限
1757	多项选择题	在GM/T 0016《智能密码钥匙密码应用接口规范》中，关于智能密码钥匙中应用的说法正确的是（）	一个设备中可以存在多个应用	不同的应用之间可以共享数据	应用由管理员PIN、用户PIN、文件和容器组成	每个应用维护各自的与管理员PIN和用户PIN相关的权限状态

1758	单项选择题	在GM/T 0016《智能密码钥匙密码应用接口规范》中，关于智能密码钥匙中应用的说法错误的是（）	一个设备中可以存在多个应用	不同的应用之间可以共享数据	应用由管理员PIN、用户PIN、文件和容器组成	每个应用维护各自的与管理员PIN和用户PIN相关的权限状态
1759	多项选择题	在GM/T 0016《智能密码钥匙密码应用接口规范》中，关于设备中的各种密钥的说法正确的是（）	签名密钥对由内部产生	加密密钥对由外部产生并安全导入	会话密钥可由内部产生或者由外部产生并安全导入	签名密钥对也可由外部产生并安全导入
1760	单项选择题	在GM/T 0016《智能密码钥匙密码应用接口规范》中，关于设备中的各种密钥的说法错误的是（）	签名密钥对由内部产生	加密密钥对由外部产生并安全导入	会话密钥可由内部产生或者由外部产生并安全导入	签名密钥对也可由外部产生并安全导入
1761	多项选择题	在GM/T 0016《智能密码钥匙密码应用接口规范》中，关于用户PIN说法正确的是	用户PIN码的解锁需要管理员权限	用户PIN码具有最大可重试次数	用户PIN码的修改需要管理员权限	PIN码长度不少于8个字节
1762	多项选择题	根据GM/T 0016《智能密码钥匙密码应用接口规范》，密钥容器存放的逻辑对象包括（）。	非对称密钥对	用户PIN	会话密钥	数字证书
1763	单项选择题	在GM/T 0017《智能密码钥匙密码应用接口数格式规范》中，规定了哪两者之间通讯的数据格式（）。	智能密码钥匙应用程序和智能密码钥匙密码应用接口之间	智能密码钥匙密码应用接口和设备（智能密码钥匙设备）驱动之间	智能密码钥匙内部	智能密码钥匙和智能密码钥匙驱动程序之间
1764	单项选择题	GM/T 0017《智能密码钥匙密码应用接口数格式规范》适用于哪种产品（）。	密码卡	签名验签服务器	智能密码钥匙	服务器密码机
1765	单项选择题	在GM/T 0017《智能密码钥匙密码应用接口数格式规范》中，规定了智能密码钥匙应用接口和设备之间的数据交换以哪种格式进行编码（）。	HEX	DER	APDU	Base64
1766	单项选择题	在GM/T 0017《智能密码钥匙密码应用接口数格式规范》中，APDU的INS字段指的是（）。	需要处理的命令	发送的数据长度字节数	期望的数据长度字节数	命令头
1767	单项选择题	在GM/T 0017《智能密码钥匙密码应用接口数格式规范》中，APDU的Lc字段指的是（）。	需要处理的命令	发送的数据长度字节数	期望的数据长度字节数	命令头

1768	单项选择题	下列哪个指令类别不属于GM/T 0017《智能密码钥匙密码应用接口数格式规范》中规定的指令类别（）。	用户管理指令	密码服务指令	访问控制指令	容器管理指令
1769	单项选择题	下列哪条指令不属于在GM/T 0017《智能密码钥匙密码应用接口数格式规范》中规定的访问控制指令（）。	DevAuth（设备认证）	VerifyAppSign（验证应用签名）	VerifyPin（校验PIN）	UnblockPin（解锁PIN）
1770	单项选择题	下列哪条指令不属于GM/T 0017《智能密码钥匙密码应用接口数格式规范》的规定的应用管理指令（）。	CreateApplication（创建应用）	EnumApplication（枚举应用）	VerifyApplication（验证应用）	CloseApplication（关闭应用）
1771	多项选择题	在GM/T 0017《智能密码钥匙密码应用接口数格式规范》中，规定了应用协议的一个步骤包含哪几个部分（）。	发送命令	接收实体处理	发回响应	设备认证
1772	多项选择题	在GM/T 0017《智能密码钥匙密码应用接口数格式规范》中，命令报文和响应报文可能出现的情况有（）。	命令报文无数据，响应报文无数据	命令报文无数据，响应报文有数据	命令报文有数据，响应报文无数据	命令报文有数据，响应报文有数据
1773	多项选择题	下列哪些指令类别属于GM/T 0017《智能密码钥匙密码应用接口数格式规范》中规定的指令类别（）。	应用管理	访问控制指令	文件管理指令	用户管理指令
1774	多项选择题	在GM/T 0017《智能密码钥匙密码应用接口数格式规范》中，GetDevInfo（获取设备信息）指令能够得到下列哪几项数据（）。	设备标签	厂商信息	容器数量	支持的算法
1775	多项选择题	下列哪些指令是GM/T 0017《智能密码钥匙密码应用接口数格式规范》中规定的应用管理指令（）。	CreateApplication（创建应用）	EnumApplication（枚举应用）	OpenApplication（打开应用）	CloseApplication（关闭应用）
1776	多项选择题	下列哪些指令是GM/T 0017《智能密码钥匙密码应用接口数格式规范》中规定的文件管理指令（）。	CreateFile（创建文件））	EnumFiles（枚举文件）	ReadFile（读取文件）	GetFileInfo（获取文件信息）
1777	多项选择题	下列哪些指令是GM/T 0017《智能密码钥匙密码应用接口数格式规范》中规定的容器管理指令（）。	CreateContainer（创建容器）	EnumContainer（枚举容器）	AddFile（增加文件）	ImportCertificate（导入数字证书）

1778	多项选择题	在GM/T 0017《智能密码钥匙密码应用接口数格式规范》中，容器中可能长期保存哪些对象（）。	加密密钥对	文件	签名证书	会话密钥
1779	判断题	在GM/T 0017《智能密码钥匙密码应用接口数格式规范》中，命令报文是从密码钥匙发送到接口设备。	正确	错误		
1780	判断题	在GM/T 0017《智能密码钥匙密码应用接口数格式规范》中，命令报文必须包含数据。	正确	错误		
1781	判断题	在GM/T 0017《智能密码钥匙密码应用接口数格式规范》中，APDU中的INS字段是指需要处理的命令。	正确	错误		
1782	判断题	在GM/T 0017《智能密码钥匙密码应用接口数格式规范》中，同一个应用下不同容器可以重名。	正确	错误		
1783	判断题	在GM/T 0017《智能密码钥匙密码应用接口数格式规范》中，命令是应用接口向设备发出的一条信息，该信息启动一个操作或请求一个应答。	正确	错误		
1784	判断题	在GM/T 0017《智能密码钥匙密码应用接口数格式规范》中，功能指的是由一个或多个命令实现的处理过程，其操作结果用于完成全部或部分交易。	正确	错误		
1785	多项选择题	在GM/T 0017《智能密码钥匙密码应用接口数据格式规范》中，文件管理指令包括（）。	创建文件	删除文件	枚举文件	文件读写
1786	单项选择题	依据GM/T 0017《智能密码钥匙密码应用接口数据格式规范》，以下那个命令不是容器管理指令（）。	创建容器	删除容器	搜索容器	枚举容器
1787	单项选择题	在GM/T 0017《智能密码钥匙密码应用接口数据格式规范》中，ImportSessionKey命令用于导入密文会话密钥，对会话密钥进行加密操作的是（）。	指定应用指定容器中的签名公钥	指定应用指定容器中的对称密钥	指定应用的指定容器中的加密公钥	指定应用指定容器中的会话密钥

1788	单项选择题	下述哪个标准中规定了操作智能密码钥匙所用的APDU命令（）。	GM/T 0016《智能密码钥匙密码应用接口规范》	GM/T 0017《智能密码钥匙密码应用接口数据格式规范》	GM/T 0018《密码设备应用接口规范》	GM/T 0019《通用密码服务接口规范》
1789	单项选择题	智能密码钥匙的用户PIN连续输入错误被锁定后，关于解锁方法，以下那个说法正确（）。	可使用正确的用户PIN对其解锁	可使用其它应用下未锁定的用户PIN对其解锁	可使用其它应用下的管理员PIN对其解锁	可使用当前应用下的管理员PIN对其解锁
1790	单项选择题	在GM/T 0048《智能密码钥匙密码检测规范》中，枚举容器检测项的检测目的是验证智能密码钥匙可以（）。	枚举出智能密码钥匙中存在的所有容器	枚举出指定应用下存在的所有容器	枚举出指定应用下存在的已导入证书的容器	枚举出指定应用下存在的有签名证书的容器
1791	单项选择题	在GM/T 0048《智能密码钥匙密码检测规范》中，解锁PIN检测项的检测目的是验证智能密码钥匙可以（）。	解锁指定应用下已锁定的管理员PIN	解锁指定应用下已锁定的用户PIN	解锁所有应用下已锁定的用户PIN	解锁所有应用下已锁定的管理员PIN
1792	单项选择题	在GM/T 0048《智能密码钥匙密码检测规范》中，导入数字证书的检测条件不包括下列哪项（）。	所需的应用和容器已打开	容器内已存在所需的密钥对	安全状态已满足	已协商会话密钥
1793	单项选择题	在GM/T 0048《智能密码钥匙密码检测规范》中，SM2验签检测规定验签使用的公钥如何获得（）。	检测样品内部生成签名密钥对	检测样品内部生成加密密钥对	密文导入加密密钥对	外部输入SM2公钥
1794	单项选择题	在GM/T 0048《智能密码钥匙密码检测规范》中，SM2生成并导出会话密钥检测，规定会话密钥应如何导出（）。	明文二进制导出	Base64编码后导出	外部公钥加密后导出	对称密钥加密后导出
1795	单项选择题	在GM/T 0048《智能密码钥匙密码检测规范》中，要求至少选择多少组参考数据（包括源数据和目标数据）（）。	1组	10组	1000组	10000组
1796	单项选择题	在GM/T 0048《智能密码钥匙密码检测规范》中，下列哪项检测要求所需的应用已打开（）。	设备认证	获取设备信息	创建应用	创建容器
1797	单项选择题	在GM/T 0048《智能密码钥匙密码检测规范》中，下列哪项检测要求所需的应用和容器已打开（）。	获取设备信息	生成随机数	枚举容器	生成SM2签名密钥对

1798	单项选择题	在GM/T 0048《智能密码钥匙密码检测规范》中，生成SM2签名密钥对的检测条件不包括下列哪项（）。	所需的应用已打开	所需的容器已打开	安全状态已满足	已导入SM2加密密钥对
1799	单项选择题	在GM/T 0048《智能密码钥匙密码检测规范》中，非对称算法性能检测要求用于检测的数据和密钥由谁来选定（）。	送检单位	检测机构	用户	设计师
1800	单项选择题	在GM/T 0048《智能密码钥匙密码检测规范》中，产品的对称算法性能应满足哪个标准中的要求（）。	GM/T 0016《智能密码钥匙密码应用接口规范》	GM/T 0017《智能密码钥匙密码应用接口数据格式规范》	GM/T 0027《智能密码钥匙技术规范》	GM/T 0028《密码模块安全技术要求》
1801	多项选择题	在GM/T 0048《智能密码钥匙密码检测规范》中，性能检测项包括以下哪些内容（）。	文件读写性能	对称算法性能	非对称算法性能	杂凑算法性能
1802	多项选择题	在GM/T 0048《智能密码钥匙密码检测规范》中，功能检测项不包括以下哪些内容（）。	容器管理	密码服务	网络连接	操作系统配置
1803	多项选择题	在GM/T 0048《智能密码钥匙密码检测规范》中，智能密码钥匙“获取PIN信息”功能输出的信息包括以下哪些内容（）。	最大重试次数	当前剩余重试次数	当前PIN是否为出厂默认PIN	用户PIN累计被修改的次数
1804	多项选择题	在GM/T 0048《智能密码钥匙密码检测规范》中，对称加密/解密功能检测要求至少检测哪几种加密模式（）。	ECB模式	CBC模式	CFB模式	CTR模式
1805	多项选择题	在GM/T 0048《智能密码钥匙密码检测规范》中，下列哪些检测项的检测条件要求所需的应用和容器已打开（）。	获取设备信息	取随机数	导入数字证书	生成SM2签名密钥对
1806	判断题	智能密码钥匙的“设备认证”是指智能密码钥匙对应用程序的认证。	正确	错误		

1807	判断题	智能密码钥匙的安全性应满足GM/T 0028《密码模块安全技术要求》，并按照GM/T 0039《密码模块安全检测要求》对其安全性进行检测和评估。	正确	错误		
1808	判断题	在GM/T 0048《智能密码钥匙密码检测规范》中，“检测方法”中描述的“检测条件”仅用于参考，不用严格执行。	正确	错误		
1809	判断题	在GM/T 0048《智能密码钥匙密码检测规范》中，单组数据加密检测在发送Encrypt指令前，要先发送EncryptInit指令。	正确	错误		
1810	判断题	在GM/T 0048《智能密码钥匙密码检测规范》中，智能密码钥匙中可以存在多个同名的应用。	正确	错误		
1811	判断题	根据GM/T 0048《智能密码钥匙密码检测规范》，在智能密码钥匙中，证书是按“应用－容器－证书”的层次关系进行管理。	正确	错误		
1812	判断题	根据GM/T 0048《智能密码钥匙密码检测规范》，智能密码钥匙的“导出数字证书”功能，可以输出容器下指定类型的数字证书和公私钥对。	正确	错误		
1813	判断题	在GM/T 0048《智能密码钥匙密码检测规范》中，只需要通过正常情况检测，异常情况检测结果不作为通过标准。	正确	错误		
1814	单项选择题	根据GM/T 0048《智能密码钥匙密码检测规范》，以下选项不是文件管理测试包含操作的为（）	创建文件	删除文件	枚举文件	重新打开文件
1815	多项选择题	根据GM/T 0048《智能密码钥匙密码检测规范》，智能密码钥匙功能检测的目的是检测智能密码钥匙实现和运行的正确性。以下选项中属于功能检测项的是（）	设备管理	应用管理	存储管理	密码服务

1816	多项选择题	根据GM/T 0048《智能密码钥匙密码检测规范》，智能密码钥匙性能检测的目的是检测智能密码钥匙文件操作和密码算法运算的效率。以下选项中属于性能检测项的是（）	文件读写性能	应用初始化性能	非对称算法性能	杂凑算法性能
1817	多项选择题	根据GM/T 0048《智能密码钥匙密码检测规范》，以下哪些选项为文件管理测试包含的操作（）	创建文件	删除文件	枚举文件	获取文件信息
1818	多项选择题	根据GM/T 0048《智能密码钥匙密码检测规范》，以下哪些为应用管理测试包含的操作（）	下载应用	枚举应用	删除应用	关闭应用
1819	多项选择题	根据GM/T 0048《智能密码钥匙密码检测规范》，以下哪些为容器管理测试包含的操作（）	创建容器	删除容器	打开容器	填充容器
1820	判断题	根据GM/T 0048《智能密码钥匙密码检测规范》，智能密码钥匙是实现密码运算、密钥管理功能，提供密码服务的终端密码设备，一般采用USB接口形态。	正确	错误		
1821	单项选择题	在GM/T 0063《智能密码钥匙应用接口检测规范》中，下列哪项检测不属于安全性检测（）。	PIN码安全要求	加密性能	设备认证	随机数安全要求
1822	单项选择题	在GM/T 0063《智能密码钥匙应用接口检测规范》中，下列哪个操作不需要验证用户PIN码（）。	导入加密密钥对	导入会话密钥	生成会话密钥并加密导出会话密钥密文	生成签名密钥对
1823	单项选择题	在GM/T 0063《智能密码钥匙应用接口检测规范》中，下列哪种密钥并不是永久存储在智能密码钥匙内，插拔后密钥丢失（）。	设备认证密钥	加密密钥对	签名密钥对	会话密钥
1824	单项选择题	在GM/T 0063《智能密码钥匙应用接口检测规范》中，智能密码钥匙内的会话密钥在（）内建立。	设备	容器	应用	文件

1825	单项选择题	在GM/T 0063《智能密码钥匙应用接口检测规范》中，下列哪种运算不需要使用加密密钥对（）。	ECC导入加密密钥对	导入会话密钥	ECC计算会话密钥	ECC产生协商数据并计算会话密钥
1826	单项选择题	在GM/T 0063《智能密码钥匙应用接口检测规范》中，下列哪项权限不属于权限使用范畴（）。	应用权限	容器权限	文件权限	会话密钥权限
1827	多项选择题	下列哪几个测试属于GM/T 0063《智能密码钥匙应用接口检测规范》的测试范围（）。	性能检测	安全性检测	接口功能检测	互操作性检测
1828	多项选择题	在GM/T 0063《智能密码钥匙应用接口检测规范》中，应用功能检测包括下列那几个测试项（）。	证书申请与下载	证书更新	数字签名	数字信封
1829	多项选择题	在GM/T 0063《智能密码钥匙应用接口检测规范》中，所涉及到的设备、容器、应用、文件和证书的包含关系描述正确的是哪几项（）。（-->表示包含）	设备-->应用-->容器-->证书	设备-->应用-->文件	设备-->容器-->应用-->证书	设备-->容器-->应用-->证书
1830	多项选择题	在GM/T 0063《智能密码钥匙应用接口检测规范》中，数字信封生成需要用到哪些功能接口（）。	导入会话密钥	生成并导出会话密钥	加密	解密
1831	多项选择题	在GM/T 0063《智能密码钥匙应用接口检测规范》中，关于设备认证密钥描述正确的是（）。	设备认证密钥在设备中是唯一的	设备认证密钥控制创建应用和删除应用的权限	设备认证密钥控制创建容器和删除容器的权限	设备认证密钥锁定后设备不可再使用
1832	多项选择题	在GM/T 0063《智能密码钥匙应用接口检测规范》中，可以通过SKF_CloseHandle关闭密码对象句柄接口关闭的句柄有（）。	会话密钥句柄	密码杂凑对象句柄	消息鉴别码对象句柄	ECC密钥协商句柄
1833	多项选择题	在GM/T 0063《智能密码钥匙应用接口检测规范》中，ECC密钥协商过程中，发起方需要调用哪些接口建立会话密钥（）。	ECC生成密钥协商参数并输出	ECC产生密钥协商数据并导出会话密钥	ECC计算会话密钥	ECC签名
1834	多项选择题	在GM/T 0063《智能密码钥匙应用接口检测规范》中，互操作性测试包括哪些功能（）。	签名验签互操作	密钥协商互操作	数字信封互操作	密钥备份操作

1835	判断题	在GM/T 0063《智能密码钥匙应用接口检测规范》中，导入数字证书接口测试过程中需要插拔设备。	正确	错误		
1836	判断题	在GM/T 0063《智能密码钥匙应用接口检测规范》中，ECC生成密钥协商参数并输出测试流程中，辅助设备承担发起方角色	正确	错误		
1837	判断题	在GM/T 0063《智能密码钥匙应用接口检测规范》中，管理员PIN码锁死后设备业务功能不可用。	正确	错误		
1838	判断题	在GM/T 0063《智能密码钥匙应用接口检测规范》中，关闭应用后，应用下的安全状态被清除。	正确	错误		
1839	判断题	在GM/T 0063《智能密码钥匙应用接口检测规范》中，送检文档不需要提供安全设计说明。	正确	错误		
1840	判断题	在GM/T 0041《智能IC卡密码检测规范》中，COS安全管理功能检测的目的是测试智能IC卡各项安全功能的运行情况，并检验实现的正确性。	正确	错误		
1841	多项选择题	在GM/T 0041《智能IC卡密码检测规范》中，COS安全管理功能检测包括的测试项有哪些（）。	外部认证测试	PIN认证测试	应用锁定测试	应用解锁测试
1842	判断题	在GM/T 0041《智能IC卡密码检测规范》中，COS安全机制检测的目的是测试智能IC卡COS为了实现安全管理而采取的手段和方法的正确性及有效性。	正确	错误		
1843	多项选择题	在GM/T 0041《智能IC卡密码检测规范》中，COS安全机制检测包括下列哪几个方面的测试（）。	报文安全传送测试	密钥安全传送测试	安全状态和访问权限测试	应用防火墙测试
1844	判断题	在GM/T 0041《智能IC卡密码检测规范》中，智能IC卡生成的随机数检测应符合GM/T 0062中B类产品的要求。	正确	错误		

1845	多项选择题	在GM/T 0041《智能IC卡密码检测规范》中，密码算法实现正确性检测包括下列哪几个方面的测试（ ）。	分组算法实现正确性测试	非对称密钥密码算法密钥生成正确性测试	杂凑算法实现正确性测试	非对称密钥密码算法数字签名及签名验证正确性测试
1846	多项选择题	在GM/T 0041《智能IC卡密码检测规范》中，密码算法实现正确性检测项中包括哪几项（ ）。	分组算法实现正确性测试	序列算法正确性测试	杂凑算法实现正确性测试	非对称密钥密码算法数字签名及签名验证正确性测试
1847	多项选择题	在GM/T 0041《智能IC卡密码检测规范》中，密码算法实现性能检测包括下列哪几个方面的性能测试（ ）。	分组密钥密码算法的加密性能测试	分组密钥密码算法的解密性能测试	非对称密钥密码算法密钥对生成性能测试	非对称密钥密码算法的加密性能测试
1848	判断题	根据GM/T 0041《智能IC卡密码检测规范》，智能IC卡安全性测试项目应遵照GM/T 0039《密码模块安全检测要求》。	正确	错误		
1849	判断题	根据GM/T 0041《智能IC卡密码检测规范》，如果送检产品有为测试独立开放的测试接口指令，需要在送检文档中加以明确说明，并在检测完毕后予以失效。	正确	错误		
1850	判断题	在GM/T 0041《智能IC卡密码检测规范》中，独立开放的测试接口只用于检测使用，不提供应用密码服务。	正确	错误		
1851	单项选择题	在GM/T 0041《智能IC卡密码检测规范》中，对外部认证进行正常测试，下列哪个步骤不正确（ ）。	使用正确的外部认证密钥进行认证，测试对象应返回认证成功的响应	在认证前操作需要安全状态的文件，测试对象应返回不满足安全状态	在操作需要安全状态的文件，测试对象应返回满足安全状态	在认证后操作需要安全状态的文件，测试对象应返回操作成功

1852	多项选择题	在GM/T 0041《智能IC卡密码检测规范》中，对外部认证进行异常测试，下列哪些步骤正确（）。	用错误的外部认证密钥去认证，测试对象应返回认证不成功并提示剩余认证次数，当剩余认证次数为零时，外部认证密钥锁定	用错误的外部认证密钥去认证，在认证后操作需要安全状态的文件，测试对象应返回不满足安全状态	用错误的密钥标识去做外部认证，测试对象应返回密钥没有找到	当测试对象存在多个外部认证密钥，成功认证外部认证密钥1，操作受外部认证密钥2保护的文件，测试对象应返回不满足安全状态
1853	多项选择题	在GMT 0041《智能IC卡密码检测规范》中，对PIN认证进行正常测试，下列哪些步骤正确（）。	使用正确的PIN进行认证，测试对象应返回认证成功响应	在认证前操作需要PIN保护的文件，测试对象应返回不满足安全状态	在GM/T 0041《智能IC卡密码检测规范》中，对外部认证进行异常测试，下列哪些步骤正确	在认证后操作需要PIN保护的文件，测试对象应返回操作成功
1854	单项选择题	在GM/T 0041《智能IC卡密码检测规范》中，对PIN重装进行异常测试，下列哪个步骤不正确（）。	用错误的填充方法计算MAC进行重装操作，测试对象应返回安全报文错误	用错误的密钥计算MAC进行重装操作，测试对象应返回安全报文错误	取随机数直接计算MAC进行重装操作，测试对象应返回该随机数	PIN的长度超出设计范围，测试对象应返回不成功
1855	多项选择题	在GM/T 0041《智能IC卡密码检测规范》中，对应用解锁进行异常测试，下列哪些步骤正确（）。	用错误的Lc计算MAC进行应用解锁操作，测试对象应返回安全报文错误	用错误的填充方法计算MAC进行应用解锁操作，测试对象应返回安全报文错误	用错误的密钥计算MAC进行应用解锁操作，测试对象应返回安全报文错误	未取随机数直接计算MAC进行应用解锁操作，测试对象应返回未取随机数
1856	单项选择题	在GM/T 0041《智能IC卡密码检测规范》中，对密钥安全传送测试，下列哪个步骤不正确（）。	用带MAC的密文方式写入外部认证密钥，并进行外部认证，测试对象应返回认证成功的响应	用带MAC的密文方式写入内部认证密钥，并进行内部认证，测试对象应返回认证成功的响应	写入PIN，并进行PIN验证，测试对象应返回认证成功的响应	用带MAC的密文方式更新外部认证密钥

1857	多项选择题	在GM/T 0041《智能IC卡密码检测规范》中，非对称密钥使用权限测试，下列哪些步骤正确（）。	未获得权限，使用非对称密钥，测试对象应返回不满足安全状态	获得权限后，可以成功使用非对称密钥运算	不应有输出明文私钥的指令	私钥删除后不能再使用
1858	多项选择题	在GM/T 0041《智能IC卡密码检测规范》中，应用防火墙测试，下列哪些步骤正确（）。	外部认证安全状态测试	PIN认证安全状态测试	应用锁定状态测试	文件更新测试
1859	判断题	在GM/T 0041《智能IC卡密码检测规范》中，对于具有随机数生成功能的智能IC卡，需要进行随机数质量检测。	正确	错误		
1860	单项选择题	在GM/T 0041《智能IC卡密码检测规范》中，非对称密钥密码算法加密解密实现正确性测试中，下列哪个步骤不正确（）。	执行非对称密钥加解密运算指令	导出公钥，对数据进行签名验证	通过加密和解密运算，生成密文结果和还原明文数据	返回运算结果，与预期结果进行比较，确认是否通过正确性验证
1861	多项选择题	在GM/T 0041《智能IC卡密码检测规范》中，分组密码算法加密解密实现正确性测试包含哪些步骤（）。	执行分组密码算法的运算指令，采用指定密钥进行运算	通过加密和解密运算，生成密文结果和还原明文数据	使用测试密钥对数据进行卡外签名	运算结果应能通过正确性验证
1862	多项选择题	根据GM/T 0041《智能IC卡密码检测规范》，分组算法加密性能测试包含哪些步骤（）。	预先产生M组（M≥1000）随机数据和随机密钥，依次通过分组算法加密指令执行加密运算	验证加密结果正确性	累积总的运算时间T	计算加密速率V，V=M/T(次/秒)
1863	多项选择题	在GM/T 0041《智能IC卡密码检测规范》中，测试对象符合下列哪些条件，可判定为合格（）。	至少应使用一种经国家密码管理主管部门批准的密码算法	如测试对象支持GMT 0041《智能IC卡密码检测规范》的6.2COS安全管理功能检测规定的全部或部分测试	应通过GMT 0041《智能IC卡密码检测规范》6.3COS安全机制检测规定的全部或部分测试	如测试对象具有RSA算法密钥对生成功能，应通过GMT 0041《智能IC卡密码检测规范》6.4 RSA密钥的素性检测规定的测试

1864	判断题	除申报安全等级为一级的智能IC卡产品外，测试对象至少应达到GM/T 0028 安全二级。	正确	错误		
1865	判断题	在GM/T 0041《智能IC卡密码检测规范》中，规定了智能IC卡产品的检测项目及检测方法。	正确	错误		
1866	判断题	在GM/T 0041《智能IC卡密码检测规范》中，数字信封是一种数据结构，包含用对称密钥加密的密文和用私钥加密的该对称密钥。	正确	错误		
1867	多项选择题	在GM/T 0041《智能IC卡密码检测规范》中，COS安全管理功能检测的目的是测试智能IC卡各项安全功能的运行情况，并检验实现的正确性。以下各项为COS安全管理功能检测的项目为（）	外部认证测试	内部认证测试	应用锁定测试	文件读写
1868	多项选择题	根据GM/T 0041《智能IC卡密码检测规范》，以下为密码算法实现正确性检测的项目是（）	非对称密钥密码算法密钥生成正确性测试	杂凑算法实现正确性测试	随机数质量测试	序列算法正确性测试
1869	多项选择题	根据GM/T 0041《智能IC卡密码检测规范》，以下为密码算法实现性能检测的项目是（）	分组密钥密码算法的解密性能测试	非对称密钥密码算法的签名验证性能测试	非对称密钥密码算法密钥对生成性能测试	随机数生成的性能测试
1870	多项选择题	根据GM/T 0041《智能IC卡密码检测规范》，以下为针对智能IC卡的检测项目是（）	智能IC卡存储容量检测	COS安全机制检测	密钥的素性检测	COS安全管理功能检测
1871	单项选择题	根据GM/T 0041《智能IC卡密码检测规范》，COS的安全机制检测的目的是测试智能IC卡COS为了实现安全管理而采取的手段和方法的正确性及有效性。以下不是COS安全机制检测项目的是（）	报文安全传送测试	密钥明文写入测试	安全状态和访问权限测试	应用防火墙测试
1872	单项选择题	在《PCI密码卡技术规范》中，下列哪项不属于PCI密码卡的功能（）。	密码运算功能	密钥管理功能	物理随机数产生功能	随主计算机可信检测功能
1873	单项选择题	在《PCI密码卡技术规范》中，PCI密码卡硬件自检不包含哪项（）。	物理噪声源	密码运算单元	静态数据完整性	用户认证数据
1874	单项选择题	在《PCI密码卡技术规范》中，PCI密码卡不适用于哪类设备（）。	密管服务器	手持式安全移动终端	云VPN	签名服务器

1875	单项选择题	在《PCI密码卡技术规范》中，下列哪项不是PCI密码卡支持的算法（ ）。	SM3	ECC	RSA	NTRU
1876	多项选择题	在《PCI密码卡技术规范》中，PCI密码卡宿主端驱动程序应实现的功能包括（ ）。	驱动程序的安装与卸载	PCI设备的打开与关闭	设备的读写操作和控制操作	应用数据的解析
1877	单项选择题	在《PCI密码卡技术规范》中，规定会话密钥长度不低于（ ）比特。	1024	512	256	128
1878	单项选择题	根据《PCI密码卡技术规范》，PCI 密码卡必须支持至少（ ）种对称密钥密码算法。	一	二	三	四
1879	多项选择题	根据《PCI密码卡技术规范》，PCI密码卡必须要支持的算法有（ ）。	对称密钥密码算法	非对称密钥密码算法	杂凑算法	随机数生成算法
1880	多项选择题	根据《PCI密码卡技术规范》，PCI密码卡可以支持的分组运算工作模式有（ ）。	ECB	CBC	OFB	CFB
1881	多项选择题	根据《PCI密码卡技术规范》，PCI密码卡包含了以下哪些密钥（ ）。	设备密钥对	用户密钥对	密钥加密密钥	会话密钥
1882	多项选择题	根据《PCI密码卡技术规范》，PCI密码卡硬件组成中以下哪些单元是不可或缺的（ ）。	实时时钟管理单元	密码运算单元	主控单元	接口单元
1883	多项选择题	根据《PCI密码卡技术规范》，PCI密码卡的密钥管理安全描述正确的是（ ）。	密码卡的密钥或密钥对的私钥由物理噪声源产生，并通过随机性检测	任何时间、任何情况下会话密钥不能以明文形式出现在硬件设备外部	用户签名密钥对可以通过有效的保护机制进行导出	硬件存储的私钥必须支持私钥访问控制码的安全访问
1884	多项选择题	在《PCI密码卡技术规范》中，PCI密码卡的设备管理安全描述正确的是（ ）	PCI密码卡需具备足够强的物理保护能力，防止底层代码被监听、盗取	在PCI密码卡正常工作时，敏感安全参数（CSP）不能以明文形式出现在硬件设备外部	驱动程序必须支持透明传输上位机和下位机的能力，不得截获、解析应用系统中的数据	设备必须要由具备核准资格的密码主管或用户才能使用
1885	多项选择题	在《PCI密码卡技术规范》中，PCI密码卡的硬件上电自检必须完成以下哪些项目（ ）。	物理噪声源是否失效	密码运算单元是否失效	静态存储数据完整性是否被破坏	在线查阅安全固件是否为最新版本

1886	单项选择题	在《PCI密码卡技术规范》中，哪项不是PCI密码卡的硬件上电自检必须完成的项目（ ）。	物理噪声源是否失效	密码运算单元是否失效	静态存储数据完整性是否被破坏	在线查阅安全固件是否为最新版本
1887	多项选择题	在《PCI密码卡技术规范》中，PCI密码卡通过API接口完成的功能检测包含哪些项目（ ）。	密码算法功能检测	密钥管理检测	程序升级接口功能检测	密码卡内敏感数据的安全保护检测
1888	多项选择题	根据《PCI密码卡技术规范》，PCI密码卡性能测试描述正确的有哪些（ ）。	每次测试应具有足够数据的数据量，防止性能波动	所有的算法性能指标都以bps为单位进行标示	对称运算性能测试时应取不同长度的数据分别进行测试	算法正确性测试时必须测试ECB、CBC、CFB、OFB等工作模式
1889	多项选择题	在《PCI密码卡技术规范》中，PCI密码卡API函数集包含以下哪些功能模块（ ）。	设备管理类函数	密钥管理类函数	算法运算类函数	文件管理类函数
1890	多项选择题	在《PCI密码卡技术规范》中，非对称密码算法的基本要求包括（ ）。	非对称密码算法应至少支持两种及以上	应提供数字签名和签名验证功能	选择支持RSA算法时，应具备2048比特及以上的模长	选择支持ECC算法时，应具备256比特及以上的模长
1891	多项选择题	根据《PCI密码卡技术规范》，PCI密码卡提供的分组密码算法必须支持哪种工作模式（ ）。	ECB	CFB	CBC	OFB
1892	判断题	根据《PCI密码卡技术规范》，PCI密码卡内的密钥均需支持定期自动更换。	正确	错误		
1893	判断题	根据《PCI密码卡技术规范》，PCI密码卡未通过上电自检时，应拒绝一切密码功能调用服务。	正确	错误		
1894	判断题	根据《PCI密码卡技术规范》，PCI 密码卡可以不支持杂凑算法。	正确	错误		
1895	判断题	根据《PCI密码卡技术规范》，PCI 密码卡可以不支持扩展密码算法。	正确	错误		
1896	判断题	根据《PCI密码卡技术规范》，PCI密码卡的软件分为三个层次：底层软件（监控软件）、驱动程序和应用编程接口。	正确	错误		

1897	判断题	根据《PCI密码卡技术规范》，驱动程序应该支持多个PCI 密码卡设备同时使用和操作的基本要求。	正确	错误		
1898	单项选择题	在GM/T 0018《密码设备应用接口规范》中，缩略词KEK表示的含义是（ ）。	椭圆曲线算法	内部加密公钥	外部加密公钥	密钥加密密钥
1899	单项选择题	在GM/T 0018《密码设备应用接口规范》中，会话密钥使用设备接口函数生成或导入，会话密钥使用什么进行检索（ ）。	接口	句柄	密钥值	设备
1900	单项选择题	在GM/T 0018《密码设备应用接口规范》中，获取私钥使用权限中的私钥访问控制码长度不少于多少字节（ ）。	2	4	6	8
1901	单项选择题	在GM/T 0018《密码设备应用接口规范》中，ECC加密数据结构为（ ）。	X分量、Y分量、明文的杂凑值、密文数据长度、密文数据	X分量、Y分量、明文的杂凑值、密文数据	X分量、Y分量、密文数据长度、密文数据	X分量、Y分量、密文数据
1902	单项选择题	在GM/T 0018《密码设备应用接口规范》定义的函数中，RSA密钥加解密数据时的填充方式为（ ）。	不填充	PKCS#1	PKCS#2	PKCS#3
1903	单项选择题	在GM/T 0018《密码设备应用接口规范》中，ECC加密数据结构中的字段M表示的含义是（ ）。	明文的杂凑值	密文数据长度	密文数据	密文的杂凑值
1904	单项选择题	在GM/T 0018《密码设备应用接口规范》定义的设备信息中，设备编号包括日期、（ ）、流水号。	版本号	设备型号	厂商名称	批次号
1905	单项选择题	在GM/T 0018《密码设备应用接口规范》中，规定密钥加密密钥长度为（ ）位。	32	64	128	256
1906	单项选择题	在GM/T 0018《密码设备应用接口规范》中，RSA公钥数据结构定义中模长变量定义的长度为（ ）。	4字节	256字节	256bit	128字节
1907	单项选择题	在符合GM/T 0018《密码设备应用接口规范》的密码设备中，用索引号0x00表示的密钥是（ ）。	密钥加密密钥	会话密钥	用户密钥	设备密钥

1908	单项选择题	在GM/T 0018《密码设备应用接口规范》中，ECC加密数据结构中的密文数据长度变量用（ ）个字节表示。	32	8	4	10
1909	单项选择题	在GM/T 0018《密码设备应用接口规范》中，ECC公钥数据结构定义中的字段不包括（ ）。	密钥位长	公钥x坐标	公钥y坐标	私钥
1910	多项选择题	根据GM/T 0018《密码设备应用接口规范》，在公钥密码基础设施应用技术体系框架中，以下哪些设备属于密码设备服务层（ ）。	密码机	密码卡	智能密码终端	扫描仪
1911	多项选择题	在GM/T 0018《密码设备应用接口规范》中，ECC签名数据结构中的字段包括哪些（ ）。	签名的r部分	签名的s部分	x分量	y分量
1912	多项选择题	在GM/T 0018《密码设备应用接口规范》中，需要分多步完成杂凑计算时，可以分为哪些步骤（ ）。	杂凑运算初始化	多包杂凑运算	杂凑运算结束	杂凑运算结果校验
1913	多项选择题	在GM/T 0018《密码设备应用接口规范》中，密码设备应有安全机制和措施，保证密钥在（ ）整个生存期间的安全，此安全机制可由设备厂商自行设计实现。	生成、安装	导入、存储	备份、恢复	销毁
1914	多项选择题	根据GM/T 0018《密码设备应用接口规范》，设计及开发的密码设备在设备状态方面，应满足（ ）。	密码设备应具有初始和就绪两个状态	未安装设备密钥的密码设备应处于初始状态，已安装设备密钥的密码设备应处于就绪状态	在初始状态下，除可读取设备信息、设备密钥的生成或恢复操作外，不能执行任何操作，生成或恢复设备密钥后，密码设备处于就绪状态	在就绪状态下，除设备密钥的生成或恢复操作外，应能执行任何操作；在就绪状态下进行的密钥操作，设备操作员应经过密码设备的认证
1915	多项选择题	在GM/T 0018《密码设备应用接口规范》中，RSA公钥数据结构定义中的字段包括（ ）。	模长	模N	公钥指数	素数p和q

1916	多项选择题	在GM/T 0018《密码设备应用接口规范》中，ECC公钥数据结构定义中的字段包括（）。	密钥位长	公钥x坐标	公钥y坐标	私钥
1917	多项选择题	在GM/T 0018《密码设备应用接口规范》中，ECC加密数据结构中包含哪些字段（）。	X分量和Y分量	明文的杂凑值	密文数据长度	密文数据
1918	多项选择题	根据GM/T 0018《密码设备应用接口规范》，密码设备在密钥方面应满足（）。	设备密钥的使用不对应用系统开放	密钥必须使用安全的方法产生并存储	在任何时间、任何情况下，除公钥外的密钥均不能以明文形式出现在密码设备外	密码设备内部存储的密钥应具备有效的密钥保护机制
1919	多项选择题	根据GM/T 0018《密码设备应用接口规范》，以下哪些属于密码设备的基本功能（）。	密钥管理	数据加密	应用管理	随机数生成
1920	多项选择题	在GM/T 0018《密码设备应用接口规范》中，ECC的私钥数据结构定义中包含（）。	密钥位长	X坐标	Y坐标	私钥K
1921	多项选择题	在GM/T 0018《密码设备应用接口规范》中，对称算法运算类函数包含（）。	对称加密：SDF_Encrypt	对称解密：SDF_Decrypt	计算MAC:SDF_CalculateMAC	验证MAC：SDF_VerifyMAC
1922	单项选择题	在GM/T 0018《密码设备应用接口规范》中提供的算法不包括（）。	非对称算法	对称算法	杂凑算法	共识算法
1923	判断题	根据GM/T 0018《密码设备应用接口规范》，函数中的会话密钥参数均以会话句柄的方式传递。	正确	错误		
1924	判断题	根据GM/T 0018《密码设备应用接口规范》，算法标识就是一种用于对密码算法进行唯一标识的符号。	正确	错误		
1925	判断题	根据GM/T 0018《密码设备应用接口规范》，当会话密钥不使用后，应该及时关闭与密码设备已建立的会话，并释放相关资源。	正确	错误		

1926	判断题	根据GM/T 0018《密码设备应用接口规范》，RSA密钥结构存储时顺序为从低到高，即密钥存放时从密钥结构数组的最低位开始，最低字节填在最低位，不足位填充数据0。	正确	错误		
1927	判断题	根据GM/T 0018《密码设备应用接口规范》，设备密钥和用户密钥存放于密钥存储区，索引号为1表示设备密钥，索引号从2开始表示用户密钥。	正确	错误		
1928	判断题	根据GM/T 0018《密码设备应用接口规范》，对称加解密函数均不对数据进行填充处理，且数据必须是指定算法分组长度的整数倍。	正确	错误		
1929	判断题	GM/T 0018《密码设备应用接口规范》标准是为密码设备服务层定义的接口规范。	正确	错误		
1930	判断题	在GM/T 0018《密码设备应用接口规范》中，ECC加密数据结构中包含明文的杂凑值字段。	正确	错误		
1931	判断题	在GM/T 0018《密码设备应用接口规范》中，产生随机数的接口支持产生自定义长度的随机数。	正确	错误		
1932	单项选择题	在GM/T 0018《密码设备应用接口规范》中，会话密钥使用设备接口函数生成或导入，使用（ ）检索。	句柄	数字	序号	字母
1933	单项选择题	在GM/T 0018《密码设备应用接口规范》中，密钥管理系统下发到设备中的ECC加密密钥对保护结构中，对称算法应采用（ ）模式。	CBC	ECB	CFB	OFB
1934	单项选择题	在GM/T 0018《密码设备应用接口规范》中，以下（ ）函数不是对称算法类函数	对称加密	对称解密	计算MAC	产生随机数
1935	多项选择题	在GM/T 0018《密码设备应用接口规范》中，密码设备一般有（ ）类型的密钥。	设备密钥	用户密钥	会话密钥	密钥加密密钥

1936	多项选择题	在GM/T 0018《密码设备应用接口规范》中，用户文件操作类函数有（ ）。	创建文件	读文件	写文件	删除文件
1937	判断题	在GM/T 0018《密码设备应用接口规范》中，密码设备的设备密钥和用户密钥都可以通过密钥管理工具，在需要使用时随时生成。	正确	错误		
1938	判断题	在GM/T 0018《密码设备应用接口规范》中，密码设备内部加密的会话密钥可以通过外部公钥进行加密转换，导出加密的会话密钥，用于数字信封转换。	正确	错误		
1939	单项选择题	在GM/T 0121《密码卡检测规范》中，下列不符合密码卡密钥使用及更新检测要求的是（ ）。	应采用访问控制技术控制内部存储密钥的访问和使用	用户密钥对和设备密钥对的私钥应具备私钥访问控制码的控制机制，防止非法使用	访问控制码的设置应由密码卡管理工具完成	访问控制码可采用口令方式，口令长度应不低于6字符，至少包含字母、数字及特殊字符中的两种
1940	单项选择题	在GM/T 0121《密码卡检测规范》中，密码卡如支持远程配置管理功能，宜符合（ ），支持或通过管理代理向上层管理应用提供设备管理应用接口。	GM/T 0018《密码设备应用接口规范》	GM/T 0028《密码模块安全技术要求》	GM/T 0039《密码模块安全检测要求》	GM/T 0050《密码设备管理 设备管理技术规范》
1941	单项选择题	在GM/T 0121《密码卡检测规范》中，若密码卡支持虚拟化功能，不同的虚拟密码卡之间应实现密钥隔离、（ ）隔离、使用隔离等功能。	芯片	接口	人员	管理
1942	单项选择题	在GM/T 0121《密码卡检测规范》中，下列不符合密码卡密钥产生及存储检测要求的是（ ）。	应支持安全存储一定数量的对称密钥和非对称密钥对	除会话密钥外的密钥均不能以明文形式出现在密码卡外	内部存储的密钥应具有权限控制机制，防止非法使用和导出	应具备有效的密钥存储保护机制，防止解剖、探测和非法读取
1943	单项选择题	在GM/T 0121《密码卡检测规范》中，密码卡出厂后，应支持使用（ ）生成会话密钥。	调试接口	管理接口	测试接口	服务接口

1944	单项选择题	在GM/T 0121《密码卡检测规范》中，密码卡密钥销毁检测要求描述错误的是（ ）。	密码卡内的密钥采用加密方式存储时，应对用于加密存储的密钥提供安全有效的销毁措施	对密码卡内以密文形式存储的密钥，在需要销毁时应提供安全有效的销毁措施	对出现在密码卡内密码运算部件中的明文密钥，使用完应及时销毁	若密码卡采用微电保护措施存储密钥，可不具备销毁密钥的触发装置
1945	单项选择题	在GM/T 0121《密码卡检测规范》中，密码卡权限管理检测要求描述正确的是（ ）。	密码卡可不支持权限配置、访问控制配置等管理功能	可不支持管理员	各角色应持有表征身份信息的硬件装置，如经商用密码检测认证的智能密码钥匙或智能IC卡等	各角色持有的表征身份信息的硬件装置，可采用口令、生物识别等技术进行身份认证
1946	单项选择题	在GM/T 0121《密码卡检测规范》中，在密码卡就绪状态下，未通过（ ），执行密钥管理操作和密码运算等安全服务操作应失败。	上电自检	周期自检	操作员身份认证	管理员身份认证
1947	单项选择题	在GM/T 0121《密码卡检测规范》中，若密码卡支持操作员角色，在就绪状态下，未通过（ ），执行密钥管理和密码运算等安全服务操作应失败。	上电自检	周期自检	操作员身份认证	管理员身份认证
1948	单项选择题	在GM/T 0121《密码卡检测规范》中，密码卡三层密钥结构中第二层密钥包括用户密钥对、密钥加密密钥和（ ）。	设备密钥对	主密钥	会话密钥	根密钥
1949	单项选择题	在GM/T 0121《密码卡检测规范》中，密码卡用户密钥对包括签名密钥对和加密密钥对，用于（ ）。	对其他密钥的管理	实现用户数字签名、签名验证，以及会话密钥的保护等	对会话密钥的保护	设备管理，不对上层应用开放
1950	多项选择题	在GM/T 0121《密码卡检测规范》中，密码卡指具有（ ）等功能的硬件板卡设备。	自身安全防护	密钥管理	密码运算功能	DDoS
1951	单项选择题	在GM/T 0121《密码卡检测规范》中，哪些不属于硬件板卡设备的功能（ ）。	自身安全防护	密钥管理	密码运算功能	DDoS

1952	多项选择题	在GM/T 0121《密码卡检测规范》中，密码卡检测项目可包括（）。	功能检测	性能检测	安全性检测	虚拟化检测
1953	多项选择题	在GM/T 0121《密码卡检测规范》中，在初始状态下，密码卡可（）。	读取设备信息	添加管理员、操作员	生成设备密钥对和保护密钥	恢复设备密钥对和保护密钥
1954	多项选择题	在GM/T 0121《密码卡检测规范》中，在就绪状态下，密码卡不能执行（）操作。	满足权限时，能够提供用户密钥管理和密码运算等功能	通过删除操作员操作使密码卡进入初始状态	生成设备密钥对和保护密钥的生成操作	恢复设备密钥对和保护密钥的操作
1955	多项选择题	在GM/T 0121《密码卡检测规范》中，密码卡应采用加密等安全方式实现（）导入。	用户密钥的加密密钥对	设备密钥的加密密钥对	密钥加密密钥	会话密钥
1956	多项选择题	在GM/T 0121《密码卡检测规范》中，密码卡的随机数质量检测应满足（）自检要求。	上电/复位自检	周期自检	单次自检	接受指令后的自检
1957	多项选择题	在GM/T 0121《密码卡检测规范》中，密码卡的性能检测应包括（）。	随机数产生性能	密钥产生性能	加解密、签名验签性能	杂凑运算性能
1958	多项选择题	在GM/T 0121《密码卡检测规范》中，下列关于密码卡驱动程序检测要求描述正确的包括（）。	在指定的操作系统中应能够正确地安装和卸载	宜支持多个密码卡设备同时使用和操作的基本要求	宜与密码卡具备安全绑定机制	不可支持多个密码卡设备同时使用和操作
1959	判断题	在GM/T 0121《密码卡检测规范》中，密码卡应支持至少一种密码杂凑算法，宜支持GB/T 15852.2规定的HMAC。杂凑函数采用SM3算法时，其实现应符合GB/T 32905要求。	正确	错误		
1960	判断题	在GM/T 0121《密码卡检测规范》中，除用户私钥、设备私钥外，其他密钥可以以明文的形式出现在密码卡外部。	正确	错误		
1961	判断题	在GM/T 0121《密码卡检测规范》中，密码卡应支持产生自身的用户密钥对和设备密钥对的加密密钥对。	正确	错误		

1962	判断题	在GM/T 0121《密码卡检测规范》中，应支持以密文等安全形式备份密码卡内部长期存储的用户密钥对和密钥加密密钥；应支持将备份的密钥恢复到密码卡；同厂商同型号的密码卡之间应支持互相备份恢复；备份恢复只能在密码卡内进行。	正确	错误		
1963	判断题	在GM/T 0121《密码卡检测规范》中，若密码卡采用微电保护措施存储密钥，应具备销毁密钥的触发装置，密码卡触发毁钥后，应立即清除微电保护存储的所有密钥，采用微电保护的密钥可以不加密。	正确	错误		
1964	判断题	在GM/T 0121《密码卡检测规范》中，密码卡应支持权限配置、访问控制配置等管理功能。应至少支持管理员。各角色应持有表征身份信息的硬件装置。	正确	错误		
1965	判断题	在GM/T 0121《密码卡检测规范》中，用户密钥对和设备密钥对的公钥不能被导出到密码卡外使用；会话密钥的导出应采用加密等安全方式实现。	正确	错误		
1966	判断题	在GM/T 0121《密码卡检测规范》中，密码卡应至少具备PCI、PCI-E、Mini PCI-E、SATUSCPCI或M.2等接口的一种，且物理接口能正常工作。	正确	错误		
1967	单项选择题	根据GM/T 0022《IPSec VPN技术规范》，在IPSec VPN中，可以为用户数据提供数据加密功能的协议是（）。	AH	ESP	SM3	ISAKMP
1968	单项选择题	根据GM/T 0022《IPSec VPN技术规范》，IPSec VPN实现的安全技术不包括（）。	隧道技术	加密技术	身份认证技术	入侵检测技术

1969	单项选择题	根据GM/T 0022《IPSec VPN技术规范》，以下关于IPSec VPN 中的 AH 协议的功能说法错误的是（ ）。	支持数据完整性校验	支持防报文重放	支持报文的加密	支持数据源验证
1970	单项选择题	根据GM/T 0022《IPSec VPN技术规范》，下列有关IPSec VPN中AH协议和ESP协议对NAT穿越支持的描述，错误的是（ ）。	在传输模式下AH协议不能穿越NAT网关	在传输模式下ESP协议能否穿越NAT网关取决于原IP	在隧道模式下AH协议不能穿越NAT网关	在隧道模式下ESP协议不能穿越NAT网关
1971	单项选择题	根据GM/T 0022《IPSec VPN技术规范》，完整的IPSecVPN密钥交换协议中，快速模式用来建立IPSec SA，对于快速模式的描述下面哪个是错误的（ ）。	基于一个ISAKMP SA的多个快速模式不能并行进行，否则会出现混乱	ISAKMP头中的MsgID唯一标识了一个正在进行中的快速模式的会话密钥协商过程	快速模式的密钥交换消息中，身份标识ID缺省定义为ISAKMP双方的IP地址，并且没有强制规定允许的协议或端口号	在通信双方之间有多条隧道同时存在的情况下，身份标识ID为对应的IPSec SA标识并规定通信数据流进入对应的隧道
1972	单项选择题	根据GM/T 0022《IPSec VPN技术规范》，关于IPSecVPN产品的密钥更新要求，以下说法错误的是（ ）。	IPSec VPN产品应具有根据时间周期和报文流量两种条件进行工作密钥和会话密钥的更新功能	IPSecVPN产品必须同时实现根据时间周期条件根据报文流量条件进行密钥更新两种能力	工作密钥的最大更新周期不大于24小时	会话密钥的最大更新周期不大于1小时
1973	单项选择题	根据GM/T 0022《IPSec VPN技术规范》，关于IPSecVPN实现的安全报文封装，以下说法错误的是（ ）。	安全报文封装协议包括AH协议和ESP协议	AH协议应与ESP协议嵌套使用	当AH与ESP协议嵌套使用时，可以启用ESP协议中的验证操作	当ESP协议单独使用时，可以协商采用可鉴别的GCM加密机制实现可鉴别能力

1974	单项选择题	根据GM/T 0022《IPSec VPN技术规范》，关于VPN产品密钥的配置，以下说法错误的是（ ）。	VPN产品所使用的设备密钥是非对称密钥，包括签名密钥对和加密密钥对	VPN产品所使用的签名密钥对由IPSec VPN产品自身产生，其公钥证书由CA认证机构签发，并导入到VPN产品中	VPN产品所使用的加密密钥对可以由CA的密钥管理系统产生，也可以由设备自身产生	VPN产品所使用的加密密钥对对应的公钥加密证书应由第三方CA认证机构签发，并导入到VPN产品中
1975	单项选择题	根据GM/T 0022《IPSec VPN技术规范》，IPSEC VPN实现中，应支持以下哪种密码算法以实现对消息源的认证（ ）。	IDEA	AES	SM3	DES
1976	多项选择题	在GM/T 0022《IPSec VPN技术规范》中，IPSec VPN安全报文协议中，包括以下哪些协议（ ）。	GRE	ESP	IKE	AH
1977	多项选择题	根据GM/T 0022《IPSec VPN技术规范》，IPSec VPN中的AH协议和ESP协议，均支持以下哪些封装模式（ ）。	隧道模式	交换模式	传输模式	路由模式
1978	单项选择题	根据GM/T 0022《IPSec VPN技术规范》，IPsec VPN在OSI模型的（ ）层进行加密。	网络层	传输层	应用层	数据链路层
1979	多项选择题	根据GM/T 0022《IPSec VPN技术规范》，下列选项中，属于IPSec VPN的ESP协议所提供服务的是（ ）。	无连接的数据完整性验证	数据源身份认证	数据报加密	防重放攻击
1980	多项选择题	根据GM/T 0022《IPSec VPN技术规范》，IPSec VPN实现支持下列哪些类别的密钥（ ）。	设备密钥	工作密钥	会话密钥	用户密钥
1981	多项选择题	根据GM/T 0022《IPSec VPN技术规范》，IPSecVPN在协商NAT穿越时，需要完成以下工作：（ ）。	判断通信双方是否支持NAT穿越	检测双方之间路径上是否存在NAT	决定如何使用UDP封装来处理NAT穿越	协商NAT穿越时使用的UDP端口号
1982	判断题	根据GM/T 0022《IPSec VPN技术规范》，在IPsecVPN的数据报文传输阶段，AH封装协议可以单独使用。	正确	错误		

1983	判断题	根据GM/T 0022《IPSec VPN技术规范》，IPSec VPN中，VPN设备的签名密钥对由设备自己生成。	正确	错误		
1984	判断题	根据GM/T 0022《IPSec VPN技术规范》，IPSec VPN中，VPN设备的加密密钥对由VPN设备自己生成。	正确	错误		
1985	判断题	根据GM/T 0022《IPSec VPN技术规范》，密钥交换协议的协议报文应使用UDP协议500或4500端口进行传输。	正确	错误		
1986	判断题	根据GM/T 0022《IPSec VPN技术规范》，快速模式用于IPSec密钥交换协议的第二阶段交换，实现通信双方IPSec安全联盟的协商，确定通信双方的IPSec安全策略及会话密钥。	正确	错误		
1987	判断题	根据GM/T 0022《IPSec VPN技术规范》，密钥交换协议消息由一个定长的消息头和固定数量的载荷组成。	正确	错误		
1988	判断题	根据GM/T 0022《IPSec VPN技术规范》，NAT_D载荷用于检测两个密钥交换通信方之间是否存在NAT设备，以及检测NAT设备的确切位置。	正确	错误		
1989	判断题	根据GM/T 0022《IPSec VPN技术规范》，在第二阶段的密钥交换过程中，快速模式交换的信息由ISAKMP SA来保护，除了ISAKMP头外，所有的载荷都处于加密状态。	正确	错误		
1990	单项选择题	在GM/T 0022《IPSec VPN技术规范》中，（ ）用于实现密钥协商。	AH协议	ESP协议	ISAKMP协议	SSL协议
1991	单项选择题	在GM/T 0022《IPSec VPN技术规范》中，（ ）模式用于IPSec协议的第一阶段交换。	主模式	快速模式	主模式或快速模式	以上都不对
1992	单项选择题	在GM/T 0022《IPSec VPN技术规范》中，（ ）协议可用于提供机密性。	AH协议	ESP协议	IKE协议	以上都可以

1993	单项选择题	在GM/T 0022《IPSec VPN技术规范》中，应使用（ ）非对称算法密钥对。	加密密钥对	签名密钥对	加密密钥对和签名密钥对	加密密钥对或签名密钥对
1994	单项选择题	在GM/T 0022《IPSec VPN技术规范》中，（ ）用于抵抗重放攻击。	安全联盟SA	安全参数索引SPI	初始化向量IV	序列号
1995	多项选择题	在GM/T 0022《IPSec VPN技术规范》中，IPSec VPN需要使用（ ）密码算法。	非对称密码算法	对称密码算法	密码杂凑算法	PRF算法
1996	多项选择题	在GM/T 0022《IPSec VPN技术规范》中，IPSec VPN需要使用（ ）类型的密钥。	设备密钥	工作密钥	会话密钥	存储密钥
1997	单项选择题	在GM/T 0022《IPSec VPN技术规范》中，密钥交换协议使用（ ）网络协议进行报文传输。	TCP协议	UDP协议	SSL协议	Http协议
1998	多项选择题	在GM/T 0022《IPSec VPN技术规范》中，AH协议可提供（ ）安全服务。	数据保密性	数据完整性	数据源鉴别	抗重放攻击服务
1999	单项选择题	在GM/T 0022《IPSec VPN技术规范》中，AH协议不提供（ ）安全服务。	数据机密性	数据完整性	数据源鉴别	抗重放攻击服务
2000	多项选择题	在GM/T 0022《IPSec VPN技术规范》中，安全联盟SA由一个三元组唯一标识，该三元组包括（ ）。	安全参数索引SPI	源IP地址	目的IP地址	安全协议标识符
2001	判断题	在GM/T 0022《IPSec VPN技术规范》中定义了OSI七层网络协议中传输层安全的协议。	正确	错误		
2002	判断题	在GM/T 0022《IPSec VPN技术规范》中定义的协议可用于建立VPN虚拟专用网。	正确	错误		
2003	单项选择题	根据GM/T 0022《IPSec VPN技术规范》，IPSec VPN不能用于实现（ ）。	网关与网关的连接	网关与端点的连接	端点与端点的连接	网关与资源的连接
2004	单项选择题	根据GM/T 0022《IPSec VPN技术规范》，IPSec VPN中的工作密钥是（ ）。	非对称密码算法密钥，用于产生会话密钥	对称密码算法密钥，用于产生会话密钥	对称密码算法密钥，用于保护会话密钥	对称密码算法密钥，用于加密数据报文

2005	单项选择题	根据GM/T 0022《IPSec VPN技术规范》，以下关于IPSec VPN会话密钥的描述，正确的是（ ）。	会话密钥由工作密钥保护，用于加密数据报文和报文MAC	会话密钥由设备密钥保护，用于加密数据报文	会话密钥由通信双方协商生成，用于保护工作密钥	会话密钥必须一次一密，每条报文均使用不同的会话密钥
2006	单项选择题	根据GM/T 0022《IPSec VPN技术规范》，IPSec VPN的工作密钥，以下描述正确的是（ ）。	应定期更换	断电时应保存	网络连接意外断开后，可以重复使用恢复连接	应进行加密保存
2007	单项选择题	在GM/T 0023《IPSec VPN网关产品规范》中规定的鉴别方式为（ ）。	公钥	预共享密钥	数字证书	口令
2008	单项选择题	在GM/T 0023《IPSec VPN网关产品规范》中，封装安全载荷ESP能提供（ ）。	可用性与完整性	完整性与机密性	授权和完整性	授权和机密性
2009	单项选择题	在GM/T 0023《IPSec VPN网关产品规范》中，密钥交换第一阶段主模式的的作用为（ ）。	实现通信双方身份的鉴别和密钥交换，得到工作密钥	实现通信双方身份的鉴别和IPSec SA的协商	实现通信双方IPSecSA的协商	实现通信双方身份的鉴别、密钥的交换以及IPSec SA的协商
2010	单项选择题	在GM/T 0023《IPSec VPN网关产品规范》中，针对管理员管理以下说法错误的是（ ）。	只能通过被授权的终端登录	应使用表明用户身份信息的硬件装置和数字证书与口令结合的方式登录	登录口令长度不小于8个字符	登录失败次数限制应小于等于5
2011	单项选择题	在GM/T 0023《IPSec VPN网关产品规范》中，以下不属于安全管理员的权限是（ ）。	设备参数配置	策略配置	密钥备份	系统备份
2012	单项选择题	在GM/T 0023《IPSec VPN网关产品规范》中，IPSec VPN网关产品工作模式的必备功能是（ ）。	隧道模式	传输模式	审计模式	安全模式
2013	单项选择题	在GM/T 0023《IPSec VPN网关产品规范》中，IPSec VPN网关产品使用错误或非法身份登录的次数限制应小于或等于多少（ ）。	12	5	10	8
2014	单项选择题	根据GM/T 0023《IPSec VPN网关产品规范》，IPSec VPN网关产品应至少具备几个工作网口（ ）。	1个	2个	3个	4个

2015	单项选择题	根据GM/T 0023《IPSec VPN网关产品规范》，IPSec VPN网关产品的平均无故障工作时间应不低于多少时（）。	1000	5000	10000	50000
2016	多项选择题	根据GM/T 0023《IPSec VPN网关产品规范》，以下对于IPSec VPN中的密钥说法错误的是（）。	设备密钥可以明文导出	工作密钥应存储于非易失性存储区	设备证书可以明文发送	设备密钥应在断电时销毁
2017	多项选择题	在GM/T 0023《IPSec VPN网关产品规范》中，设备自检应包含（）。	检查密码运算部件正确性	检查存储密钥的完整性	检查硬件随机数产生部件正常工作	检查身份鉴别介质及其接口
2018	多项选择题	在GM/T 0023《IPSec VPN网关产品规范》中，设备密钥的用途包括以下哪些（）。	数字签名	数字信封	业务数据加密	身份鉴别
2019	多项选择题	在GM/T 0023《IPSec VPN网关产品规范》中，IPSec提供了哪些安全服务（）。	数据源鉴别	完整性保护	载荷机密性	抗重放攻击
2020	多项选择题	根据GM/T 0023《IPSec VPN网关产品规范》，以下哪些属于IPSec VPN产品性能参数（）。	加解密吞吐	加解密时延	每秒新建隧道数	最大并发隧道数
2021	多项选择题	根据GM/T 0023《IPSec VPN网关产品规范》，IPSec VPN使用的密钥种类包括（）。	设备密钥	工作密钥	会话密钥	根密钥
2022	多项选择题	下面（）属于IPSec VPN安全策略五元组的内容。	源IP地址	目的IP地址	源传输层端口	目的传输层端口
2023	判断题	GM/T 0023《IPSec VPN网关产品规范》要求工作密钥的最大更新周期不大于48小时。	正确	错误		
2024	判断题	根据GM/T 0023《IPSec VPN网关产品规范》，IPSec VPN中安全报文封装协议分为AH协议和ESP协议，两者都可独立使用。	正确	错误		
2025	判断题	根据GM/T 0023《IPSec VPN网关产品规范》，IPSec中对称密码算法应使用ECB模式。	正确	错误		

2026	判断题	根据GM/T 0023《IPSec VPN网关产品规范》，IPSec VPN网关产品工作模式应支持隧道模式和传输模式，其中传输模式是可选功能，仅用于网关实现。	正确	错误		
2027	判断题	根据GM/T 0023《IPSec VPN网关产品规范》，IPSec VPN的工作密钥和会话密钥应在设备重启时存储到非易失性存储区以便快速恢复。	正确	错误		
2028	判断题	根据GM/T 0023《IPSec VPN网关产品规范》，IPSec VPN网关产品每次启动均应该进行自检。	正确	错误		
2029	判断题	根据GM/T 0023《IPSec VPN网关产品规范》，IPSec VPN网关产品应具备密钥交换功能。	正确	错误		
2030	判断题	根据GM/T 0023《IPSec VPN网关产品规范》，AH协议用于加密和认证IP数据报。	正确	错误		
2031	判断题	根据GM/T 0023《IPSec VPN网关产品规范》，IPSec VPN的所有密码运算应都在独立的密码部件中进行。	正确	错误		
2032	单项选择题	在GM/T 0023《IPSec VPN网关产品规范》中，（）密钥用于保护会话密钥协商的过程。	签名密钥对	加密密钥对	设备密钥	工作密钥
2033	单项选择题	在GM/T 0023《IPSec VPN网关产品规范》中，IPSec VPN网关产品的实体认证应采用（）方式。	口令	MAC消息认证码	数字证书	对称加密
2034	单项选择题	在GM/T 0023《IPSec VPN网关产品规范》中，工作密钥的最大更新周期应不大于（）。	1小时	24小时	7天	一个月
2035	单项选择题	根据GM/T 0023《IPSec VPN网关产品规范》，IPSec VPN网关产品应能够在（）协议单独使用时支持NAT穿越。	AH	ESP	IKE	Kebores
2036	多项选择题	GM/T 0023《IPSec VPN网关产品规范》规定了IPSec VPN网关产品的（）等有关内容。	功能要求	硬件要求	软件要求	安全性要求

2037	多项选择题	根据GM/T 0023《IPSec VPN网关产品规范》，IPSec VPN网关产品应提供日志功能，日志内容包括（ ）。	操作行为	安全事件	异常事件	会话密钥
2038	多项选择题	根据GM/T 0023《IPSec VPN网关产品规范》，设备密钥的管理包括（ ）等操作。	生成	导入	备份	恢复
2039	多项选择题	在GM/T 0023《IPSec VPN网关产品规范》中，设备自检包括（ ）等操作。	关键部件的正确性检查	密钥等敏感信息的完整性检查	随机数生成部件的检查	CPU等物理部件的常规检查
2040	判断题	根据GM/T 0023《IPSec VPN网关产品规范》，IPSec VPN网关产品开机后应重新发起密钥协商。	正确	错误		
2041	单项选择题	根据GM/T 0024《SSL VPN技术规范》，SSL VPN协议中密码规格变更协议用于通知。	协议的变更	安全参数的变更	性能的变更	物理环境的变更
2042	单项选择题	根据GM/T 0024《SSL VPN技术规范》，SSL VPN协议中握手所需要的随机数长度为多少字节（ ）。	14	32	28	64
2043	单项选择题	根据GM/T 0024《SSL VPN技术规范》，SSL VPN协议中数据扩展函数（P_hash）采用了哪个方式（ ）。	SM4	HMAC	SHA256	SHA1
2044	单项选择题	根据GM/T 0024《SSL VPN技术规范》，SSL VPN协议中ECC 和 ECDHE的算法为（ ）。	RSA	SM1	SM2	SM9
2045	单项选择题	根据GM/T 0024《SSL VPN技术规范》，SSL VPN协议中IBC和IBSDH的算法为（ ）。	RSA	SM1	SM2	SM9
2046	单项选择题	根据GM/T 0024《SSL VPN技术规范》，SSL VPN协议中用于数据加密和校验的密钥是（ ）。	主密钥	工作密钥	服务端密钥	客户端密钥
2047	单项选择题	根据GM/T 0024《SSL VPN技术规范》，SSL VPN协议中，用于生成主密钥是（ ）。	主密钥	预主密钥	服务端密钥	客户端密钥
2048	多项选择题	根据GM/T 0024《SSL VPN技术规范》，SSL VPN 中非对称密码算法包括（ ）。	SM2	SM9	ElGamal	RSA

2049	多项选择题	根据GM/T 0024《SSL VPN技术规范》，SSL VPN 中非对称密码算法用于（）。	身份鉴别	数字签名	密钥交换	数据报文加密
2050	单项选择题	根据GM/T 0024《SSL VPN技术规范》，SSL VPN中分组密码算法用了哪些加密模式（）。	ECB	CBC	CTR	OFB
2051	多项选择题	根据GM/T 0024《SSL VPN技术规范》，SSL VPN协议主要包括以下哪些（）。	记录层协议	握手协议	报警协议	密码规格变更协议
2052	多项选择题	根据GM/T 0024《SSL VPN技术规范》，SSL VPN协议中记录层协议包括以下哪些（）。	传输数据的分段	压缩及解压缩	加密及解密	完整性校验
2053	多项选择题	根据GM/T 0024《SSL VPN技术规范》，SSL VPN中报警消息的长度为两个字节，分别为（）。	报警次数	报警级别	报警内容	报警时间
2054	多项选择题	根据GM/T 0024《SSL VPN技术规范》，下列哪些是标准规定的密码套件（）。	ECC_SM4_SM3	IBC_SM4_SM3	ECDHE_SM4_SM3	RSA_SM4_SM3
2055	多项选择题	根据GM/T 0024《SSL VPN技术规范》，SSL VPN中握手协议用于（）。	身份鉴别	访问控制	安全参数协商	加解密业务数据
2056	多项选择题	根据GM/T 0024《SSL VPN技术规范》，SSL VPN中握手协议族包括哪些（）。	密码规格变更协议	报警协议	握手协议	加密协议
2057	判断题	根据GM/T 0024《SSL VPN技术规范》，SSL VPN 中非对称密码算法用于业务数据加密。	正确	错误		
2058	判断题	根据GM/T 0024《SSL VPN技术规范》，SSL VPN中预主密钥的作用是用于生成主密钥。	正确	错误		
2059	判断题	根据GM/T 0024《SSL VPN技术规范》，SSL VPN中报警协议用于关闭通知和对错误进行报警。	正确	错误		
2060	判断题	根据GM/T 0024《SSL VPN技术规范》，SSL VPN中记录层协议中压缩算法不能为空。	正确	错误		

2061	判断题	根据GM/T 0024《SSL VPN技术规范》，SSL VPN中记录层可以将数据分成2^16字节长度。	正确	错误		
2062	判断题	根据GM/T 0024《SSL VPN技术规范》，SSL VPN中，RSA_SM4_SM3是一个合规的密码套件。	正确	错误		
2063	判断题	根据GM/T 0024《SSL VPN技术规范》，SSL VPN中签名密钥对是由自身密码模块产生。	正确	错误		
2064	判断题	根据GM/T 0024《SSL VPN技术规范》，SSL VPN中支持流密码加密。	正确	错误		
2065	单项选择题	在GM/T 0024《SSL VPN技术规范》中，（ ）协议用于传输数据的分段、压缩及解压缩、加密及解密、完整性校验等。	握手协议	密码规格变更协议	网关到网关协议	记录层协议
2066	单项选择题	在GM/T 0024《SSL VPN技术规范》中，哪一方的实体鉴别是必备的（ ）。	客户端	服务端	客户端和服务端都是必备的	客户端和服务端都不是必备的
2067	多项选择题	在GM/T 0024《SSL VPN技术规范》中，主密钥的生成与（ ）等素材有关。	预主密钥	客户端随机数	服务端随机数	常量字符串
2068	多项选择题	在GM/T 0024《SSL VPN技术规范》中，工作密钥包括（ ）。	签名密钥对	加密密钥对	数据加密密钥	校验密钥
2069	多项选择题	在GM/T 0024《SSL VPN技术规范》中，SSL协议包括（ ）。	握手协议	记录层协议	IKE协议	报警协议
2070	多项选择题	在GM/T 0024《SSL VPN技术规范》中，一个密码套件包括（ ）。	密钥交换算法	加密算法	校验算法	压缩算法
2071	判断题	在GM/T 0024《SSL VPN技术规范》中规定，一个SSL会话只能用于一个连接。	正确	错误		
2072	单项选择题	根据GM/T 0024《SSL VPN技术规范》，SSL VPN的会话与网络连接的关系为（ ）。	一个会话只能对应一个连接，一个连接只能对应一个会话	一个会话只能对应一个连接，一个连接可以对应多个会话	一个连接只能对应一个会话，一个会话可以对应多个连接	一个连接可以对应多个会话，一个会话可以对应多个连接

2073	单项选择题	根据GM/T 0024《SSL VPN技术规范》，SSL VPN握手协议的第一步是（）。	客户端发起，第一个消息是ClientHello	客户端发起，第一个消息是ClientRequest	服务端发起，第一个消息是ServerHello	服务端发起，第一个消息是ServerChallenge
2074	单项选择题	根据GM/T 0024《SSL VPN技术规范》，SSL VPN的工作密钥包括（）。	加密密钥和签名密钥	加密密钥和校验密钥	会话密钥和签名密钥	会话密钥和校验密钥
2075	单项选择题	根据GM/T 0024《SSL VPN技术规范》，关于SSL VPN的工作密钥更新的规定是（）。	当会话持续进行时，工作密钥一直有效	工作密钥根据时间周期进行更新为必备功能	无需根据报文流量更新工作密钥	必须同时设置会话持续时间限值和流量限值。当两个限值均被超过时，会话密钥必须更新
2076	单项选择题	根据GM/T 0025-2014《SSL VPN网关产品规范》，以下哪类信息不能被导入到SSL VPN网关产品中（）。	签名证书	加密证书	签名密钥对的私钥	加密密钥对的私钥
2077	单项选择题	根据GM/T 0025-2014《SSL VPN网关产品规范》，SSL VPN网关产品硬件应符合（）对硬件模块物理安全的规定。	GM/T 0028《密码模块安全技术要求》	GM/T 0023《IPSec VPN网关产品规范》	GM/T 0005《随机性检测规范》	GM/T 0026《安全认证网关产品规范》
2078	单项选择题	根据GM/T 0025-2014《SSL VPN网关产品规范》，SSL VPN网关产品软件升级应具备修复安全漏洞的能力，在升级前应对升级包文件进行（）。	机密性校验	病毒扫描	完整性校验	功能校验
2079	单项选择题	根据GM/T 0025-2014《SSL VPN网关产品规范》，SSL VPN网关产品的平均无故障工作时间应不低于（）小时。	7*24	100	1024	10000
2080	单项选择题	根据GM/T 0025-2014《SSL VPN网关产品规范》，SSL VPN服务端产品管理员应持有表征用户身份信息的硬件装置与登录口令相结合登录系统，使用错误口令或非法身份登录的次数限制应小于或等于（）。	3次	5次	8次	10次

2081	单项选择题	根据GM/T 0025-2014《SSL VPN 网关产品规范》，SSL VPN 网关产品工作密钥产生后应保存在（）中，达到其更新条件后应立即更换，在连接断开、设备断电时应销毁。	易失性存储器	非易失性存储器	USBKEY	光盘
2082	多项选择题	根据GM/T 0025-2014《SSL VPN 网关产品规范》，SSL VPN 网关产品工作模式有哪几种模式（）。	客户端-服务端模式	网关-网关模式	客户端-客户端模式	独立服务端模式
2083	多项选择题	根据GM/T 0025-2014《SSL VPN 网关产品规范》，SSL VPN 网关产品应具有细粒度的访问控制功能,对于网络访问至少应控制到（）。	IP 地址	MAC地址	协议	端口
2084	多项选择题	根据GM/T 0025-2014《SSL VPN 网关产品规范》，SSL VPN产品应采用分权管理的机制，涉及的管理员角色包括（）。	超级管理员	系统管理员	安全管理员	系统审计员
2085	多项选择题	根据GM/T 0025-2014《SSL VPN 网关产品规范》，SSL VPN使用的非对称密码算法主要用于（）。	认证	数据加密	数字签名	数字信封
2086	多项选择题	根据GM/T 0025-2014《SSL VPN 网关产品规范》，SSL VPN 网关应具有信息传递功能，用户访问 HTTP 应用时，系统在完成相应的身份鉴别后，把验证结果、用户的基本信息插入到 HTTP 请求中传送给后台的应用系统，应用系统通过标准的 HTTP 操作即可获取信息，并基于该信息作相应的访问控制以及进行相应的业务审计。获取的信息包括（）。	用户 IP地址	用户证书的关键信息	用户MAC地址	终端信息
2087	多项选择题	根据GM/T 0025-2014《SSL VPN 网关产品规范》，SSL VPN 网关产品应提供日志记录、查看和导出功能，日志内容包括（）。	管理员操作行为，包括用户管理、登录认证、系统配置、密钥管理操作	用户访问行为，包括用户、时间、访问资源、结果	异常事件，包括认证失败、非法访问异常事件的记录	系统运行期间的输出，包括数据接收、数据处理、数据回执的处理信息

2088	判断题	根据GM/T 0025-2014《SSL VPN 网关产品规范》，SSL VPN 网关产品应具有实体鉴别的功能，鉴别方式采用数字证书或账号口令的鉴别机制。	正确	错误		
2089	判断题	根据GM/T 0025-2014《SSL VPN 网关产品规范》，SSL VPN 网关对于网关-网关模式，工作密钥最长时间更新周期不超过 8小时。	正确	错误		
2090	判断题	根据GM/T 0025-2014《SSL VPN 网关产品规范》，SSL VPN产品的加密密钥对由外部密钥管理机构产生并由外部认证机构签发签名证书。	正确	错误		
2091	判断题	根据GM/T 0025-2014《SSL VPN 网关产品规范》，SSL VPN 网关产品硬件应符合 GM/T 0028《密码模块安全技术要求》对硬件模块物理安全的规定。	正确	错误		
2092	判断题	根据GM/T 0025-2014《SSL VPN 网关产品规范》，SSL VPN网关产品管理员应通过数字证书认证进行鉴别，并通过加密通道对SSL VPN 网关进行管理配置。	正确	错误		
2093	判断题	根据GM/T 0025-2014《SSL VPN 网关产品规范》，SSL VPN 网关产品的初始化过程中涉及的系统配置、密钥的生成和管理、管理员的产生均应由厂家完成。	正确	错误		
2094	单项选择题	根据GM/T 0025《SSL VPN网关产品规范》，SSL VPN网关应具有（ ）功能，通过协商产生工作密钥。	密钥交换	安全报文传输	数据压缩	身份鉴别
2095	单项选择题	根据GM/T 0025《SSL VPN网关产品规范》，SSL VPN网关产品设备密钥的签名密钥对应由（ ）产生。	外部产生	产品自身产生	外部或产品自身产生	以上都不对
2096	多项选择题	在GM/T 0025《SSL VPN网关产品规范》中，SSL VPN网关产品的日志管理功能包括（ ）。	记录	查看	修改	导出

2097	单项选择题	在GM/T 0025《SSL VPN网关产品规范》中，SSL VPN网关产品的日志管理功能不包括（ ）。	记录	查看	修改	导出
2098	多项选择题	在GM/T 0025《SSL VPN网关产品规范》中，SSL VPN网关产品自检的必选项包括（ ）。	算法正确性	密钥完整性	随机数可靠性	软件功能模块
2099	单项选择题	根据GM/T 0025-2014《SSL VPN 网关产品规范》，SSL VPN网关与客户端握手过程中如何鉴别对方身份（ ）。	通过非对称密码算法	通过对称密码算法	通过密码杂凑算法	通过MAC算法
2100	单项选择题	在GM/T 0026-2014《安全认证网关产品规范》中，虚拟专用网络是以下哪个选项的缩写（ ）。	SSL	NAT	VPN	IPSec
2101	单项选择题	在GM/T 0026-2014《安全认证网关产品规范》中，安全认证网关是采用（ ）技术对用户进行身份鉴别。	数字签名	用户名口令	指纹	人脸识别
2102	单项选择题	根据GM/T 0026-2014《安全认证网关产品规范》，安全认证网关的部署模式分为串联和（ ）两种方式。	门卫式	交叉	云部署	并联
2103	单项选择题	根据GM/T 0026-2014《安全认证网关产品规范》，密钥交换产生的工作密钥及会话密钥在安全认证网关每次启动时均应（ ）。	置零	加载	加密存储	读取至内存
2104	单项选择题	根据GM/T 0026-2014《安全认证网关产品规范》，遵循 IPSec 协议的安全认证网关产品性能参数包括加解密吞吐量、加解密时延、加解密丢包率、（ ）和最大并发隧道数。	每秒新建连接数	每秒丢包率	每秒新建隧道数	每秒销毁隧道数
2105	单项选择题	根据GM/T 0026-2014《安全认证网关产品规范》，所有的配置数据应保证其在设备中的（ ）、可靠性。	完整性	机密性	不可否认性	可追溯性
2106	单项选择题	根据GM/T 0026-2014《安全认证网关产品规范》，管理员通过（ ）进行鉴别，登录到安全认证网关进行管理配置，管理员通过被授权的终端登录到安全认证网关进行相应的配置操作。	生物识别	数字签名	动态口令	扫码

2107	多项选择题	根据GM/T 0026-2014《安全认证网关产品规范》，安全认证网关应确保设备密钥得到安全保护，工作密钥和会话密钥不存放在（ ）中。	硬盘	内存	易失性存储介质	非易失性存储介质
2108	多项选择题	根据GM/T 0026-2014《安全认证网关产品规范》，安全认证网关产品应提供日志记录、查看和导出功能。日志内容包括（ ）。	操作行为	加解密内容	用户访问行为	安全事件
2109	判断题	根据GM/T 0026-2014《安全认证网关产品规范》，在安全认证网关中，非对称密码算法用于认证、数字签名和数据加密。	正确	错误		
2110	判断题	根据GM/T 0026-2014《安全认证网关产品规范》，对于遵循 SSL VPN协议的安全认证网关，应在每次SSL握手时，鉴别最终用户的证书及签名，并进行证书黑名单（CRL）的检查。	正确	错误		
2111	判断题	根据GM/T 0026-2014《安全认证网关产品规范》，用户访问同一台网关保护的多个应用时，应只存在一次身份鉴别过程。	正确	错误		
2112	判断题	根据GM/T 0026-2014《安全认证网关产品规范》，对于遵循 SSL VPN协议的安全认证网关，对于客户端-服务端模式，工作密钥的最长更新周期不超过1天。	正确	错误		
2113	判断题	根据GM/T 0026-2014《安全认证网关产品规范》，对于遵循 IPSec 协议的安全认证网关产品来说，NAT 穿越是必备功能。	正确	错误		
2114	判断题	根据GM/T 0026-2014《安全认证网关产品规范》，安全认证网关在安全报文传输阶段应具有对抗重放攻击的功能。	正确	错误		

2115	判断题	根据GM/T 0026-2014《安全认证网关产品规范》，为方便设备上线后的调试和问题排查，安全认证网关在产品定型后，应提供可供调试、跟踪的外部接口。	正确	错误		
2116	判断题	根据GM/T 0026-2014《安全认证网关产品规范》，安全认证网关产品的初始化，系统配置、参数的配置、安全策略的配置、密钥的生成和管理、管理员的产生均应由生产厂商完成。	正确	错误		
2117	单项选择题	在GM/T 0026《安全认证网关产品规范》中，NAT穿越对于（ ）产品是必备检测。	IPSec协议的安全认证网关	SSL协议的安全认证网关	A和B都是必备的	A和B都不是必备的
2118	单项选择题	在GM/T 0026《安全认证网关产品规范》中，安全认证网关的（ ）应在产品定型后封闭。	通信接口	管理接口	调试接口	以上都可以不封闭
2119	多项选择题	在GM/T 0026《安全认证网关产品规范》中，采用SSL协议的安全认证网关产品的性能检测主要包括（ ）。	最大并发用户数	最大并发连接数	每秒新建连接数	吞吐率
2120	多项选择题	在GM/T 0026《安全认证网关产品规范》中，采用IPSec协议的安全认证网关产品的性能检测主要包括（ ）等方面。	加解密吞吐率	加解密时延	加解密丢包率	最大并发隧道数
2121	多项选择题	在GM/T 0026《安全认证网关产品规范》中，安全认证网关的哪些初始化操作应由用户完成。	安全策略的配置	密钥的生成	管理员的产生	设备零部件的组装
2122	判断题	在GM/T 0026《安全认证网关产品规范》中，安全认证网关的部署模式分为物理串联和物理并联两种方式。	正确	错误		
2123	判断题	在GM/T 0026《安全认证网关产品规范》规定的物理串联部署方式中，用户可以不经过网关访问受保护的应用。	正确	错误		

2124	单项选择题	根据GM/T 0049《密码键盘密码检测规范》，密码键盘安全等级共分为几级（）。	4级	3级	5级	2级
2125	单项选择题	根据GM/T 0049《密码键盘密码检测规范》，密码键盘对称算法检测不包括以下哪项内容（）。	加密检测	解密检测	签名检测	MAC检测
2126	单项选择题	根据GM/T 0049《密码键盘密码检测规范》，密码键盘非对称算法检测不包括以下哪项内容（）。	签名检测	验签检测	MAC检测	加密检测
2127	多项选择题	根据GM/T 0049《密码键盘密码检测规范》，密码键盘上电自检必须包括以下哪些项（）。	软件/固件完整性检测	随机数自检检测	非对称算法自检检测	关键功能自检检测
2128	单项选择题	根据GM/T 0049《密码键盘密码检测规范》，PIN正确情况检测中，哪些数据是无需提供的（）。	PIN数据块加密密钥	PIN码	主账号	MAC密钥
2129	单项选择题	根据GM/T 0049《密码键盘密码检测规范》，密码键盘PIN数据块异常检测异常条件不包括哪一项（）。	错误的PIN数据块加密密钥	错误误的PIN码	错误的主账号	错误的密码算法
2130	单项选择题	根据GM/T 0049《密码键盘密码检测规范》，密码键盘检测内容不包括下列哪项（）。	密码算法检测	运行环境检测	算法性能检测	设备安全性检测
2131	单项选择题	根据GM/T 0049《密码键盘密码检测规范》，密码键盘哪个安全等级最高（）。	1级	2级	3级	4级
2132	单项选择题	根据GM/T 0049《密码键盘密码检测规范》，已知结果检测，检测机构需提供指定的至少多少组明文与密文的测试数据对（）。	1000	100	10	1
2133	单项选择题	根据GM/T 0049《密码键盘密码检测规范》，下列哪项不是密码键盘对称算法稳定性检测方法（）。	已知结果检测	多数据块检测	蒙特卡洛检测	单数据块检测
2134	单项选择题	根据GM/T 0049《密码键盘密码检测规范》，密码键盘的外部认证指的是以下哪一个（）。	密码键盘的身份认证	公钥认证	私钥认证	证书认证

2135	单项选择题	根据GM/T 0049《密码键盘密码检测规范》，密码键盘运行前条件自检检测是指下面哪一项（）。	对密码键盘软件和固件的完整性进行的检测	在密码键盘运行之前，当规定的检测条件出现时，由密码键盘执行的功能正确性检测	对密码键对密码键盘生成的PIN数据块正确性进行的检测	对密码键对密码键盘中对称密码算法加密和解密进行的功能正确性检测
2136	多项选择题	根据GM/T 0049《密码键盘密码检测规范》，软件/固件完整性检测，密码键盘可以采用哪些方法进行（）。	采用MAC	采用核准的数字签名	采用文档和源代码的审查	没有方法检测
2137	多项选择题	根据GM/T 0049《密码键盘密码检测规范》，MAC算法检测的步骤包括以下哪些内容（）。	检测机构将测试数据发送给密码键盘	密码键盘利用检测机构提供的MAC参数对接收到的数据进行加密运算	将密码键盘生成的MAC与检测机构的MAC进行比对	用指定的密钥对测试数据进行解密运算，密码键盘返回运算结果
2138	多项选择题	根据GM/T 0049《密码键盘密码检测规范》，随机数质量检测的检测步骤包括哪些（）。	输入测试数据（明文/密文，密钥，以及模式所需的初始向量IV）	输出加密结果/解密结果；	用密码键盘产生随机数，直至采集够128MB	用GB/T 32915-2016规定的方法对随机数进行检测，并判定是否通过检测
2139	多项选择题	根据GM/T 0049《密码键盘密码检测规范》，环境失效保护检测的通用要求有哪些（）。	对于安全1级、2级的密码键盘，不要求具有环境失效保护（EFP）特性或者经过环境失效检测（EFT）	如果温度或电压超出密码键盘的正常运行范围，则保护电路应关闭键盘，防止继续运行或立即置零所有敏感信息	安全3级的密码键盘应具有EFP特性或经过EFT，安全4级的密码键盘应具有EFP特性	密码键盘加密一组已知的数据，把得到的密文送给检测平台
2140	多项选择题	根据GM/T 0049《密码键盘密码检测规范》，对称密码算法稳定性检测主要包括哪些检测内容（）。	密钥生成检测	已知结果检测	多数据块检测	蒙特卡洛检测

2141	多项选择题	根据GM/T 0049《密码键盘密码检测规范》，非对称密码算法验签检测的检测步骤包括以下哪些内容（）。	由检测机构提供200组正确的测试数据（如：正确的签名结果、签名者信息、待签名消息和密钥对）	输入测试数据，密码键盘对输入的数据进行验签	密码键盘返回200组正确的验签结果	将输出的杂凑值与检测机构的数据进行比对
2142	多项选择题	根据GM/T 0049《密码键盘密码检测规范》，安全功能检测中安全1级包括哪些检测（）。	检测密码键盘部件是否由产品级部件组成以及部件是否采用了标准钝化技术	检测密码键盘在运行维护功能运行时，密码键盘是否能被操作员按规定程序置零，或由密码键盘自动置零	检测密码键盘的外壳是否为金属或硬质塑料的产品级外壳	检测密码键盘是否能防止错误注入攻击
2143	多项选择题	在GM/T 0049《密码键盘密码检测规范》规定的安全功能检测中，下面哪些检测项目是安全3级的检测要求（）。	检测密码键盘是否存在通风孔或缝，若不存在则继续检测	通过安全2级的检测	检测密码键盘是否具有EFP特性或经过EFT。如果是则继续检测	检测密码键盘在温度超出运行，存放和分发的预期温度范围时，外壳是否维持强度或硬度特征。如果是则继续检测
2144	多项选择题	根据GM/T 0049《密码键盘密码检测规范》，下面哪些是需要提交送检的技术文档（）。	密码键盘产品规格说明书	密码自检测或自评估报告	与密码实现和使用相关的硬件说明	密码键盘接口说明
2145	判断题	在GM/T 0049《密码键盘密码检测规范》的随机数自检检测中，送检单位应提交随机数自检的自检文档和随机数自检源代码。	正确	错误		
2146	判断题	在GM/T 0049《密码键盘密码检测规范》的关键功能自检测试中，送检单位应提交关键功能自检测试的源代码。	正确	错误		

2147	判断题	根据GM/T 0049《密码键盘密码检测规范》，对称密码算法自检检测是可选测试项。	正确	错误		
2148	判断题	在GM/T 0049《密码键盘密码检测规范》周期自检检测中，检测人员通过文档和源代码的审查，确认源代码实现的周期自检测试和文档描述是否一致。	正确	错误		
2149	判断题	在GM/T 0049《密码键盘密码检测规范》中，密码键盘支持其他PIN数据块填充格式，送检单位不需提供PIN数据块填充格式说明文档。	正确	错误		
2150	判断题	根据GM/T 0049《密码键盘密码检测规范》，如果密码键盘同时还支持其他MAC算法，送检单位必须提供MAC算法具体计算的说明文档。	正确	错误		
2151	判断题	在GM/T 0049《密码键盘密码检测规范》MAC算法检测中，密码键盘利用送检单位提供的MAC参数对接收到的数据进行加密运算。	正确	错误		
2152	判断题	在GM/T 0049《密码键盘密码检测规范》MAC计算性能检测中，检测人员操作密码键盘用密钥对分好的每组数据依次进行一次MAC运算，记录运算完成的总时间T，只需要检测一次，根据公式就可以计算出用来评估性能的运算速率。	正确	错误		
2153	判断题	根据GM/T 0049《密码键盘密码检测规范》，安全1级密码键盘部件由产品级部件组成以及部件采用了标准钝化技术。	正确	错误		

2154	单项选择题	根据GM/T 0049-2016《密码键盘密码检测规范》，有一款键盘通过了基本检测项目的全部测试，其安全要求检测的结果为：安全功能检测2级\密钥安全2级\安全状态3级\ 密码算法4级，该键盘的最终评级是几级（ ）。	1级	2级	3级	4级
2155	单项选择题	根据GM/T 0049-2016《密码键盘密码检测规范》，在对称密码算法稳定性检测时，以下哪一项是错误的（ ）。	已知结果检测	多数据块检测	蒙特卡洛检测	算法正确性检测
2156	单项选择题	根据GM/T 0049-2016《密码键盘密码检测规范》，关于密钥置零，以下错误的是（ ）。	安全2级的密码键盘，未受保护的密钥和使用完毕的临时密钥会置零，且输出完成状态指示	对安全2级的密码键盘进行非法操作，密钥会置零	安全2级的密码键盘，键盘的置零操作不可中断	安全3级的密码键盘，置零操作过程中，不可恢复已被置零数据。
2157	多项选择题	在GM/T 0049-2016《密码键盘密码检测规范》中，环境失效保护要求（ ）。	对于安全1级、2级的密码键盘，不要求具有环境失效保护（EFP）特性或者经过环境失效检测（EFT）	安全3级的密码键盘应具有EFP特性或经过EFT，安全4级的密码键盘应具有EFP特性	如果温度或电压超出密码键盘的正常运行范围，则保护电路应关闭键盘，防止继续运行或立即置零所有敏感信息	如果键盘检测到外部暴力拆解、强力振动、强电磁干扰，则保护电路应关闭键盘，防止继续运行或立即置零所有敏感信息。
2158	多项选择题	根据GM/T 0049-2016《密码键盘密码检测规范》，密钥安全检测包括（ ）。	生成密钥	密钥存储	密钥输入与输出	密钥置零

2159	多项选择题	根据GM/T 0049-2016《密码键盘密码检测规范》，能达到安全4级，最低的要求应包括（）。	基本测试项目全部通过	基本测试项目没有通过（某些可选测试项可以不测）	安全要求检测项目全部通过4级检测。	安全要求中的非关键要求可不通过4级检测
2160	判断题	根据GM/T 0049-2016《密码键盘密码检测规范》，密码键盘的安全等级代表了其所具有的安全能力的高低。其中安全1级最低，安全4级最高。	正确	错误		
2161	判断题	根据GM/T 0049-2016《密码键盘密码检测规范》，对称密码算法加密和解密检测，包括两个测试内容：加密检测和解密检测。	正确	错误		
2162	单项选择题	根据GM/T 0045《金融数据密码机技术规范》，根据GM/T 0045《金融数据密码机技术规范》，金融数据密码机中在业务功能中，针对密钥和PIN的计算，算法工作模式均采用（）模式。	ECB	CBC	CFB	OFB
2163	单项选择题	根据GM/T 0045《金融数据密码机技术规范》，金融数据密码机中对称密码算法的工作模式应至少包括哪两种（）。	ECB和OFB模式	ECB和CBC模式	CBC和OFB模式	CBC和CFB模式
2164	单项选择题	根据GM/T 0045《金融数据密码机技术规范》，公钥算法在金融数据密码机中的作用不包括（）。	签名验签	密码信封	密钥分发	数据摘要
2165	单项选择题	根据GM/T 0045《金融数据密码机技术规范》，金融数据密码机产生并导出SM2密钥对时，公钥以明文形式导出，私钥经哪一类密钥加密后导出（）。	本地主密钥LMK	终端主密钥TMK	终端PIN加密密钥TPK	终端MAC计算密钥TAK
2166	单项选择题	根据GM/T 0045《金融数据密码机技术规范》，金融数据密码机中随机产生SM2密钥对，密钥可以保存在密码机中，保存在密码机中的密钥以（）方式访问。	句柄	接口	索引	设备

2167	单项选择题	根据GM/T 0045《金融数据密码机技术规范》，金融数据密码机的最顶层密钥是（ ）。	本地主密钥LMK	PIN加密密钥PIK	区域主密钥ZMK	区域PIN加密密钥ZPK
2168	单项选择题	根据GM/T 0045《金融数据密码机技术规范》，金融数据密码机提供设备自检功能，自检项不包括（ ）。	算法正确性	随机数	密钥存储	用户状态
2169	单项选择题	根据GM/T 0045《金融数据密码机技术规范》，金融数据密码机应采用不少于几个硬件物理噪声源产生随机数（ ）。	1个	2个	3个	4个
2170	单项选择题	根据GM/T 0045《金融数据密码机技术规范》，金融数据密码机的密钥机制为（ ）层。	二层	三层	四层	根据应用需求确定
2171	单项选择题	根据GM/T 0045《金融数据密码机技术规范》，金融数据密码机的平均无故障工作时间应不低于（ ）小时。	1000	5000	10000	50000
2172	单项选择题	根据GM/T 0045《金融数据密码机技术规范》，金融数据密码机在出厂检测时，有（ ）项不通过检测标准，则告警检测不合格。	1	2	3	4
2173	单项选择题	根据GM/T 0045《金融数据密码机技术规范》，金融数据密码机中的主密钥只能在（ ）时才能导出密码机。	系统备份	密钥交换	设备认证	数据加密
2174	单项选择题	根据GM/T 0045《金融数据密码机技术规范》，金融数据密码机中保护数据密钥的安全传输、分发的是（ ）。	主密钥	次主密钥	工作密钥	共享密钥
2175	单项选择题	根据GM/T 0045《金融数据密码机技术规范》，金融数据密码机的主密钥和次主密钥在注入密码机时，应至少由（ ）名以上的授权管理员在注入现场共同完成。	1	2	3	4
2176	多项选择题	根据GM/T 0045《金融数据密码机技术规范》，金融数据密码机支应持以下哪些密钥类型（ ）。	区域主密钥ZMK	PIN加密密钥PIK	终端PIN加密密钥TPK	区域PIN加密密钥ZPK

2177	多项选择题	根据GM/T 0045《金融数据密码机技术规范》，金融数据密码机采用分层密码机制，分别为（）。	主密钥	次主密钥	数据密钥	设备密钥
2178	多项选择题	根据GM/T 0045《金融数据密码机技术规范》，金融数据密码机对称密码算法的工作模式至少应包括哪两种工作模式（）。	ECB	CBC	CRT	OFB
2179	多项选择题	根据GM/T 0045《金融数据密码机技术规范》，金融数据密码机应提供设备自检功能，设备自检项包括（）。	算法正确性检查	随机数发生器检查	存储密钥完整性检查	敏感数据完整性检查
2180	多项选择题	根据GM/T 0045《金融数据密码机技术规范》，金融数据密码机应具备（）的备份/恢复功能。	主密钥	次主密钥	数据密钥	会话密钥
2181	多项选择题	根据GM/T 0045《金融数据密码机技术规范》，金融数据密码机中，主密钥在备份介质中存储应遵循（）的原则。	多段保存	多人方式保存	每段分人保存	分别保存
2182	多项选择题	根据GM/T 0045《金融数据密码机技术规范》，金融数据密码机提供的日志包括（）。	操作日志	交易日志	管理日志	运行日志
2183	多项选择题	根据GM/T 0045《金融数据密码机技术规范》，金融数据密码机根据应用的不同，应用编程接口可划分为（）。	磁条卡应用	IC卡应用	基础密码运算服务	设备管理服务
2184	多项选择题	根据GM/T 0045《金融数据密码机技术规范》，（）属于金融数据密码机功能检测中的强制检测项目。	初始化检测	随机数检测	访问控制检测	设备管理检测
2185	判断题	根据GM/T 0045《金融数据密码机技术规范》，数据密钥是实际金融业务中使用的工作密钥，。可以以明文的形式出现在密码机外	正确	错误		
2186	判断题	根据GM/T 0045《金融数据密码机技术规范》，金融数据密码机的初始化可以由厂商进行。	正确	错误		

2187	判断题	根据GM/T 0045《金融数据密码机技术规范》，金融数据密码机应具有自检功能，自检项不通过不能继续进行工作。	正确	错误		
2188	判断题	根据GM/T 0045《金融数据密码机技术规范》，金融数据密码机的启动、停止和配置可以由任何人员进行操作。	正确	错误		
2189	判断题	金融数据密码机采用三层密钥机制，分别为主密钥、次主密钥和数据密钥三层。	正确	错误		
2190	判断题	根据GM/T 0045《金融数据密码机技术规范》，金融数据密码机设备主密钥明文存储时，应采用微电保护方式存储。	正确	错误		
2191	判断题	根据GM/T 0045《金融数据密码机技术规范》，金融数据密码机设备自检不通过时应报警但可以继续工作。	正确	错误		
2192	判断题	根据GM/T 0045《金融数据密码机技术规范》，金融数据密码机在判定随机数发生器失效后，还可以对外提供服务。	正确	错误		
2193	判断题	根据GM/T 0045《金融数据密码机技术规范》，备份后的密钥恢复操作只能在金融数据密码机能进行。	正确	错误		
2194	判断题	GM/T 0045《金融数据密码机技术规范》标准规定了同厂家的不同型号的金融数据密码机之间应能够互相备份恢复。	正确	错误		
2195	判断题	根据GM/T 0045《金融数据密码机技术规范》，金融数据密码机的厂商可任意定义错误码。	正确	错误		
2196	判断题	GM/T 0045《金融数据密码机技术规范》标准规定密码运算检测方法是将密码机的密码运算结果与已知的正确结果进行比较，如果相同，则测试通过；否则，测试失败。	正确	错误		

2197	判断题	GM/T 0045《金融数据密码机技术规范》标准规定密码运算检测时针对对称密码算法的检测只需检测一种工作模式即可。	正确	错误		
2198	单项选择题	根据GM/T 0045《金融数据密码机技术规范》，为保证访问控制的安全性，金融数据密码机的启动、停止和配置只能由（）完成。	维护员	审计员	操作员	授权管理员
2199	单项选择题	根据GM/T 0045《金融数据密码机技术规范》，金融数据密码机的安全性设计应符合规范（）。	GM/T 0050《 密码设备管理 设备管理技术规范》	GM/T 0046《金融数据密码机检测规范》	GM/T 0028《密码模块安全技术要求》	GM/T 0039《密码模块安全检测要求》
2200	单项选择题	根据GM/T 0045《金融数据密码机技术规范》，（）是金融数据密码机的核心功能，保护密钥在产生、安装、存储、使用、备份、恢复整个生命周期安全。	设备管理	随机数产生	密钥管理	访问控制
2201	多项选择题	根据GM/T 0045《金融数据密码机技术规范》，金融数据密码机应在启动过程中进行自检，在其它时间也可进行周期或手动自检，自检项目有（）。	密码运算部件等关键部件进行正确性检查	随机数进行随机性检查	存储的密钥等敏感信息进行完整性检查	网络连接情况检查
2202	判断题	根据GM/T 0045《金融数据密码机技术规范》，金融数据密码机中的密钥应分层保护，保护原则为“自下向上逐层保护”。	正确	错误		
2203	判断题	根据GM/T 0045《金融数据密码机技术规范》，金融数据密码机应设置独立的服务接口和管理接口，分别用于密码服务和设备管理，接口的功能不能交叉混用。	正确	错误		
2204	单项选择题	根据GM/T 0046《金融数据密码机检测规范》，金融数据密码机应具备至少（）个服务端口，（）个管理端口	1，1	1，2	2，1	2，2

2205	单项选择题	根据GM/T 0046《金融数据密码机检测规范》，如果没有进行初始化配置，则金融数据密码机启动时应通过（ ）进行报警，提示用户进行初始化。	指示灯	报警声	指示灯或报警声	指示灯和报警声
2206	单项选择题	根据GM/T 0046《金融数据密码机检测规范》，金融数据密码机生成的（ ）作为测试样本，进行随机数质量检测。	PIN转加密结果	随机比特流	鉴别数据	加密数据
2207	单项选择题	根据GM/T 0046《金融数据密码机检测规范》，金融数据密码机的关键安全操作应由（ ）授权后才能进行。	管理员	审计员	用户	操作员
2208	单项选择题	根据GM/T 0046《金融数据密码机检测规范》，金融数据密码机随机数自检中的使用检测包括周期检测与（ ）。	上电检测	出厂检测	初始化检测	单次检测
2209	单项选择题	根据GM/T 0046《金融数据密码机检测规范》，金融数据密码机手工自检通过（ ）执行。	管理界面	预设代码	业务接口调用	外部管理指令输入
2210	单项选择题	根据GM/T 0046《金融数据密码机检测规范》，如果自检失败，金融数据密码机应报告检测结果并且（ ）对外提供密码服务。	询问后停止	停止	继续	有限的提供
2211	单项选择题	根据GM/T 0046《金融数据密码机检测规范》，金融数据密码机的（ ）接口测试正确，认为检测通过。	IC卡接口、磁条卡接口、密码管理接口	状态类接口、设备类接口、管理类接口	密码服务类接口、密码管理类接口	业务类接口、状态类接口、管理类接口
2212	单项选择题	根据GM/T 0046《金融数据密码机检测规范》，如果没有进行初始化配置，则此时金融数据密码机不能提供（ ）。	管理服务	密码服务	显示版本号服务	状态查询服务
2213	单项选择题	根据GM/T 0046《金融数据密码机检测规范》，经过初始化配置的金融数据密码机，可（ ）进入工作状态。	手动	自动	重启后	延迟十分钟后

2214	单项选择题	根据GM/T 0046《金融数据密码机检测规范》，金融数据密码机的管理工具按照指定的参数生成主密钥，应以安全的方法存储到（ ）中。	硬盘	移动介质	内存	安全介质
2215	单项选择题	根据GM/T 0046《金融数据密码机检测规范》，金融数据密码机的如果密钥存储采用微电保护存储方式，密码机（ ）情况下打开机箱，密钥需被自动销毁。	加电	不加电	加电或不加电	加电和不加电
2216	单项选择题	根据GM/T 0045《金融数据密码机技术规范》，金融数据密码机采用（ ）层密钥机制。	一	二	三	四
2217	单项选择题	根据GM/T 0046《金融数据密码机检测规范》，金融数据密码机的密钥管理工具不应提供（ ）功能。	产生主密钥	导入主密钥	导出主密钥	查询主密钥
2218	多项选择题	根据GM/T 0046《金融数据密码机检测规范》，金融数据密码机初始化应支持（ ）。	未初始化状态指示	管理员生成	服务端口配置	管理端口配置
2219	多项选择题	根据GM/T 0046《金融数据密码机检测规范》，金融数据密码机至少应支持的密码算法包括（ ）。	SM2密码算法	SM3密码算法	SM4密码算法	SM9密码算法
2220	多项选择题	根据GM/T 0046《金融数据密码机检测规范》，金融数据密码机的关键安全操作应由管理员授权后执行，这些安全操作包括（ ）。	密钥注入	密钥备份与恢复	密钥导入与导出	密钥销毁
2221	多项选择题	根据GM/T 0046《金融数据密码机检测规范》，金融数据密码机的日志内容应包括（ ）的记录。	登录认证	系统配置	密钥管理	非法访问
2222	多项选择题	根据GM/T 0045《金融数据密码机技术规范》，金融数据密码机密钥不允许以明文形态完整地出现在密码机之外，在通过（ ）等形式输出时，应具有完整的管理措施保证非授权人员不能接触到明文密钥。	密码信封	码单	IC卡	智能密码钥匙
2223	多项选择题	根据GM/T 0046《金融数据密码机检测规范》，金融数据密码机对称算法的工作模式至少应包括（ ）。	ECB模式	CBC模式	OFB模式	CFB模式

2224	多项选择题	根据GM/T 0046《金融数据密码机检测规范》，金融数据密码机的管理权限应有明确的角色划分，至少具备（ ）。	管理员	审计员	用户	操作员
2225	多项选择题	根据GM/T 0046《金融数据密码机检测规范》，金融数据密码机的随机数检测内容包括（ ）。	出厂检测	上电检测	使用检测	关机检测
2226	多项选择题	根据GM/T 0046《金融数据密码机检测规范》，金融数据密码机设备自检应包括（ ）。	密码算法正确性检查	关键部件正确性检测	存储密钥和数据完整性检查	随机数发生器检查
2227	多项选择题	根据GM/T 0046《金融数据密码机检测规范》，以下（ ）属于金融数据密码机性能测试内容。	PIN加密性能测试	PIN转加密性能测试	MAC计算性能测试	SM4 ARQC验证性能测试
2228	多项选择题	根据GM/T 0046《金融数据密码机检测规范》，金融数据密码机应提供日志审计功能，包括（ ）。	日志记录	日志查看	日志导入	日志导出
2229	判断题	根据GM/T 0046《金融数据密码机检测规范》，金融数据密码机密钥管理包括密钥的产生、注入、导入/导出、备份/恢复、查询和销毁。	正确	错误		
2230	判断题	根据GM/T 0046《金融数据密码机检测规范》，金融数据密码机管理工具应具备以下功能：产生主密钥、导入主密钥、查询主密钥、销毁密钥。	正确	错误		
2231	判断题	根据GM/T 0046《金融数据密码机检测规范》，金融数据密码机可不具备真随机数生成功能。	正确	错误		
2232	判断题	根据GM/T 0046《金融数据密码机检测规范》，金融数据密码机的密钥的产生和初始PIN的产生可不使用真随机数。	正确	错误		
2233	判断题	根据GM/T 0046《金融数据密码机检测规范》，金融数据密码机宜具有备份内部存储密钥到安全介质的功能。	正确	错误		

2234	判断题	根据GM/T 0046《金融数据密码机检测规范》，金融数据密码机管理操作授权要有严格的身份认证机制。	正确	错误		
2235	判断题	根据GM/T 0046《金融数据密码机检测规范》，金融数据密码机服务端口的授权访问机制是可选的。	正确	错误		
2236	判断题	根据GM/T 0046《金融数据密码机检测规范》，金融数据密码机设备安全性测试应遵照GM/T 0039《密码模块安全检测要求》。	正确	错误		
2237	判断题	根据GM/T 0046《金融数据密码机检测规范》，当调用金融数据密码机业务报文接口时，如调用环境和调用过程不正确，应返回相应的错误代码。	正确	错误		
2238	判断题	根据GM/T 0046《金融数据密码机检测规范》，金融数据密码机如果密钥存储采用微电保护存储方式，应具备密钥自毁机制。	正确	错误		
2239	单项选择题	在GM/T 0046《金融数据密码机检测规范》中，在对金融数据密码机进行外观结构检查时，根据产品的物理参数，对金融数据密码机的外观、尺寸、内部部件及附件进行检查。以下不属于必备部件或端口是（ ）。	电源指示灯	具备至少1个服务端口	具备至少1个管理端口	USB接口
2240	单项选择题	在GM/T 0046《金融数据密码机检测规范》中，金融数据密码机设备安全性检测遵照（ ）。	GM/T 0039《密码模块安全检测要求》	GM/T 0046《金融数据密码机检测规范》	GM/T 0028《密码模块安全技术要求》	GM/T 0059《服务器密码机检测规范》
2241	多项选择题	在GM/T 0046《金融数据密码机检测规范》中，金融数据密码机检测项目中，如果任意一项必须具备的功能项检测结果不合格，判定为产品不合格。以下选项属于检测合格必须具备的功能项是（ ）。	密码运算检测合格	送检文档符合检测要求	设备安全性检测符合GM/T 0039	随机数检测符合检测要求

2242	多项选择题	在GM/T 0046《金融数据密码机检测规范》中规定的金融数据密码机检测项目主要包括（）。	设备外观和结构检查	功能检测	性能检测	环境适应性和稳定性检测
2243	多项选择题	在GM/T 0046《金融数据密码机检测规范》中，金融数据密码机功能检测主要有（）。	初始化和访问控制检测	密码运算和密钥管理检测	数据报文接口和随机数检测	日志审计和设备自检检测
2244	多项选择题	在GM/T 0046《金融数据密码机检测规范》中，金融数据密码机检测规范中，要求对密码机进行性能检测，检测项目有（）。	对称密码算法性能	非对称密码算法性能	杂凑算法性能	常用计算方法性能(PIN、MAC)
2245	判断题	根据GM/T 0046《金融数据密码机检测规范》，如果没有进行过初始化配置，金融数据密码机启动时应通过指示灯和声音进行报警，提示用户进行初始化，此时金融数据密码机不能提供密码服务。	正确	错误		
2246	判断题	根据GM/T 0046《金融数据密码机检测规范》，金融数据密码机在进行密码运算功能检测时，需预置测试密钥，测试密钥由送检厂商来确定。	正确	错误		
2247	判断题	在GM/T 0046《金融数据密码机检测规范》中，密码机应具备密钥自毁机制。如果密钥存储采用微电保护存储方式，密码机加电与不加电两种情况下打开机箱，密钥都必须能被自动销毁。	正确	错误		
2248	单项选择题	根据GM/T 0030《服务器密码机技术规范》，非对称运算算法性能单位统一为（）。	tps	Mb/s	KB/s	kb/s
2249	单项选择题	根据GM/T 0030《服务器密码机技术规范》，以下哪一项不属于服务器密码机的密钥管理功能（）。	产生	安装	派生	存储
2250	单项选择题	根据GM/T 0030《服务器密码机技术规范》，以下关于SM2非对称密钥公钥和私钥的说法错误的是（）。	非对称密码算法中可以公开的密钥称为公钥	非对称密码算法中只能由拥有者使用的不公开的密钥称为私钥	一对SM2密钥由公钥和私钥组成	SM2私钥可以用来做对称运算

2251	单项选择题	根据GM/T 0030《服务器密码机技术规范》，服务器密码机对外应该提供（ ）和管理接口。	服务接口	输入接口	输出接口	统计接口
2252	单项选择题	根据GM/T 0030《服务器密码机技术规范》，已安装设备密钥的服务器密码机应处于（ ）。	启动状态	运行状态	输出状态	就绪状态
2253	单项选择题	根据GM/T 0030《服务器密码机技术规范》，密钥加密密钥是定期更换的对称密钥，用于在预分配密钥情况下，对（ ）的保护。	会话密钥	设备密钥	非对称密钥	管理密钥
2254	单项选择题	根据GM/T 0030《服务器密码机技术规范》，服务器密码机必须至少支持三层密钥结构：管理密钥、用户密钥/设备密钥/密钥加密密钥、（ ）。	非对称密钥	对称密钥	会话密钥	管理密钥
2255	多项选择题	根据GM/T 0030《服务器密码机技术规范》，服务器密码机的随机数发生器应支持什么检测方式（ ）。	使用检测	出厂检测	上电检测	故障检测
2256	多项选择题	根据GM/T 0030《服务器密码机技术规范》，服务器密码机的远程管理功能只能用于远程监控，包括（ ）。	参数查询	密钥备份	状态查询	密钥恢复
2257	多项选择题	根据GM/T 0030《服务器密码机技术规范》，服务器密码机的日志内容包括（ ）。	登录认证	系统配置	密钥管理	业务数据
2258	多项选择题	根据GM/T 0030《服务器密码机技术规范》，密码运算检测的范围包括（ ）。	对称密码算法	非对称密码算法	杂凑算法	共识算法
2259	多项选择题	根据GM/T 0030《服务器密码机技术规范》，服务器密码机在密钥管理方面，应满足以下哪些要求（ ）。	管理密钥的使用可以对应用系统开放	除公钥外，所有密钥均不能以明文形式出现在服务器密码机外	服务器密码机内部存储的密钥应具备防止解剖、探测和非法读取有效的密钥保护机制	服务器密码机内部存储的密钥应具备防止非法使用和导出的权限控制机制

2260	判断题	根据GM/T 0030《服务器密码机技术规范》，服务器密码机在对称密码算法上必须至少支持 SM4 分组密码算法,包括电子密本(ECB)、密码分组链接(CBC)、输出反馈(OFB)三种模式。	正确	错误		
2261	判断题	根据GM/T 0030《服务器密码机技术规范》，服务器密码机应具有密钥的产生、安装、存储、使用、销毁以及备份和恢复等功能。	正确	错误		
2262	判断题	根据GM/T 0030《服务器密码机技术规范》，服务器密码机必须至少支持三层密钥结构：管理密钥、用户密钥/设备密钥/密钥加密密钥、会话密钥。	正确	错误		
2263	判断题	根据GM/T 0030《服务器密码机技术规范》，服务器密码机应提供日志记录、查看和导出功能。	正确	错误		
2264	判断题	根据GM/T 0030《服务器密码机技术规范》，用户密钥分为签名密钥和加密密钥,签名密钥由服务器密码机生成，加密密钥通过密钥管理系统下发到设备中。	正确	错误		
2265	判断题	根据GM/T 0030《服务器密码机技术规范》，服务器密码机必须至少支持SM1、SM2、SM3、SM4四种算法。	正确	错误		
2266	判断题	根据GM/T 0030《服务器密码机技术规范》，对称密码算法的加解密性能单位为：tps（次/每秒）。	正确	错误		
2267	单项选择题	根据GM/T 0030-2014《服务器密码机技术规范》，服务器密码机必须至少支持几层密钥结构（）。	1	2	3	4
2268	多项选择题	根据GM/T 0030-2014《服务器密码机技术规范》，服务器密码机必须至少支持哪几层密钥结构（）。	管理密钥	用户密钥	出厂密钥	会话密钥

2269	多项选择题	根据GM/T 0030-2014《服务器密码机技术规范》，服务器密码机日志的内容包括哪些（）。	登录认证	异常事件	系统配置	与设备管理中心连接情况
2270	多项选择题	根据GM/T 0030-2014《服务器密码机技术规范》，以下属于服务器密码机可提供的算法工作模式的有（）。	CRL	OFB	CBC	ECB
2271	多项选择题	根据GM/T 0030-2014《服务器密码机技术规范》，服务器密码机需要满足以下哪几项功能要求（）。	非对称密码运算	对称密码运算	密钥管理	随机数生成
2272	判断题	根据GM/T 0030-2014《服务器密码机技术规范》，服务器密码机平均无故障工作时间应不低于7*24小时。	正确	错误		
2273	判断题	根据GM/T 0030-2014《服务器密码机技术规范》，服务器密码机应提供日志记录、查看和导出的功能。	正确	错误		
2274	判断题	根据GM/T 0030-2014《服务器密码机技术规范》，服务器密码机可以仅提供服务接口。	正确	错误		
2275	单项选择题	根据GM/T 0059《服务器密码机检测规范》，服务器密码机首次加电启动，应自动进入（）状态，此时密码机不能提供密码服务。	自检	初始	运行	就绪
2276	单项选择题	根据GM/T 0059《服务器密码机检测规范》，经过初始化配置的密码机加电启动，可自动进入（）状态，密码机方可提供密码服务。	自检	初始	运行	就绪
2277	单项选择题	根据GM/T 0059《服务器密码机检测规范》，在设备随机数质量检测中的使用检测阶段，单次检测中根据实际应用时每次所采随机数的长度不应低于多少比特（）。	64	128	192	256
2278	单项选择题	根据GM/T 0059《服务器密码机检测规范》，管理密钥应在（）态由服务器密码机厂家提供的管理工具生成或安装，且安全地存储在密码机内部。	自检	初始	运行	就绪

2279	单项选择题	根据GM/T 0059《服务器密码机检测规范》，密码机的远程管理接口检测不包括（ ）。	初始化设备管理环境	导出设备证书	获取私钥	设置告警信息为已处理
2280	单项选择题	根据GM/T 0059《服务器密码机检测规范》，批量获取设备属性值属于（ ）检测项目。	设备远程管理接口检测	设备访问控制检测	设备应用接口检测	设备配置管理检测
2281	单项选择题	根据GM/T 0059《服务器密码机检测规范》，服务器密码机常规检测环境中，服务器密码机与服务器之间的通信协议是（ ）。	TCP/IP	NTP	FTP	SNMP
2282	多项选择题	根据GM/T 0059《服务器密码机检测规范》，服务器密码机的日志内容可以包括（ ）。	管理员操作行为，包括登录认证、系统配置、密钥管理等操作	异常事件，包括认证失败、非法访问等异常事件的记录	如与设备管理中心连接，则对相应操作进行记录	对应用接口中密钥管理相关调用记录日志
2283	多项选择题	根据GM/T 0059《服务器密码机检测规范》，密码机权限配置宜具备（ ）。	管理员、安全员、操作员三类角色管理	管理员负责安全员和操作员的添加、修改和注销	安全员负责操作员的权限管理以及日志审计	操作员负责密码机的常规配置操作
2284	多项选择题	根据GM/T 0059《服务器密码机检测规范》，服务器密码机应具备哪些主要部件或接口（ ）。	应支持状态指示灯，目测状态灯能区分出正常工作状态和故障状态	应支持电源指示灯，目测能区分设备是否上电	应支持至少2个RJ45网络接口	可支持USB接口
2285	多项选择题	根据GM/T 0059《服务器密码机检测规范》，管理应支持哪几个主要功能（ ）。	应支持密钥管理功能，密钥管理功能应包括密钥产生、密钥存储、密钥备份、密钥恢复和密钥销毁等子功能；	应支持设备唯一标识符查询	应支持设备状态管理功能，设备状态管理应包括设备状态查询功能，宜包括硬件部件状态、软件状态和版本状态等状态管理功能	宜支持日志管理，日志管理功能应包含日志记录、日志查询和日志导出等功能
2286	多项选择题	根据GM/T 0059《服务器密码机检测规范》，服务器密码机的设备配置管理可分为（ ）。	权限配置	网络配置	访问控制配置	应用配置

2287	判断题	根据GM/T 0059《服务器密码机检测规范》，服务器密码机采用远程管理方式时，管理机与密码机之间应建立安全通道。	正确	错误		
2288	判断题	根据GM/T 0059《服务器密码机检测规范》，密码机应支持密钥备份和密钥恢复，备份文件应以明文形式存放在安全的存储介质中。	正确	错误		
2289	判断题	根据GM/T 0059《服务器密码机检测规范》，服务器密码机应具备自检状态和待机状态两种状态，且只能由待机状态向自检状态转换。	正确	错误		
2290	判断题	根据GM/T 0059《服务器密码机检测规范》，就绪状态的密码机只能通过触发毁钥机制并断电重启后，才能再次进入初始状态，不能通过管理界面、控制口、人机交互部件或其他方式将密码机的状态从就绪状态转换到初始状态。	正确	错误		
2291	判断题	根据GM/T 0059《服务器密码机检测规范》，登录服务器密码机应具备完善的身份认证机制，不同的管理操作应有不同的操作权限，但允许有一个权限最高管理员可进行全部操作。	正确	错误		
2292	判断题	根据GM/T 0059《服务器密码机检测规范》，服务器密码机应支持管理功能和密码服务功能，不同功能采用分开的物理接口访问。	正确	错误		
2293	判断题	根据GM/T 0059《服务器密码机检测规范》，密码机权限配置中的角色管理包括管理员、安全员、操作员三类角色。	正确	错误		
2294	判断题	根据GM/T 0059《服务器密码机检测规范》，密码机的每一项性能检测都应进行多次检测，结果取去掉最大值和最小值后的中位数。	正确	错误		

2295	判断题	服务器密码机随机数质量检测中如果有1项不通过检测标准，则告警检测不通过。	正确	错误		
2296	判断题	根据GM/T 0059《服务器密码机检测规范》，服务器密码机应具备随机数生成功能，应至少具备1个独立的物理噪声源。	正确	错误		
2297	单项选择题	根据GM/T 0059-2018《服务器密码机检测规范》，服务器密码机应具备完善的密钥管理功能，应至少支持（ ）层密钥结构。	一	二	三	四
2298	多项选择题	根据GM/T 0059-2018《服务器密码机检测规范》，服务器密码机状态包括（ ）。	初始状态	就绪状态	未初始化状态	正常状态
2299	多项选择题	根据GM/T 0059《服务器密码机检测规范》，服务器密码机应支持自检功能，自检应包括（ ）。	上电/复位自检	软件自检	周期自检	接受指令后的自检
2300	多项选择题	根据GM/T 0059《服务器密码机检测规范》，服务器密码机权限配置宜具备哪些类角色管理（ ）。	管理员	安全员	统计员	操作员
2301	多项选择题	根据GM/T 0059《服务器密码机检测规范》，服务器密码机的 API 接口检测应包括以下哪几类（ ）。	设备管理类函数	对称算法运算类函数	用户文件操作类函数	杂凑运算类函数
2302	判断题	根据GM/T 0059《服务器密码机检测规范》，对于存储在服务器密码机内部的公钥，应持有正确的私钥访问控制码才能使用。	正确	错误		
2303	判断题	根据GM/T 0059《服务器密码机检测规范》，未经过初始化配置的服务器密码机加电启动，可自动进入就绪状态，服务器密码机可提供密码服务。	正确	错误		
2304	判断题	根据GM/T 0059《服务器密码机检测规范》，自检成功，服务器密码机应进入就绪状态；自检失败，服务器密码机应记录日志并报警，并立即停止对外提供密码服务。	正确	错误		

2305	判断题	根据GM/T 0029-2014《签名验签服务器技术规范》，在签名验签服务器中，应该支持用户证书、根证书或者证书链的导入，导入时应对证书的有效性进行验证。	正确	错误		
2306	判断题	根据GM/T 0029-2014《签名验签服务器技术规范》，签名验签服务器能够配置时间源服务器，自动同步时间。	正确	错误		
2307	单项选择题	根据GM/T 0029《签名验签服务器技术规范》，签名验签服务器是用于服务端的，为应用实体提供基于PKI体系和数字证书的数字签名、验证签名等运算功能的服务器，下列哪项不是签名验签服务器保证关键业务信息的功能（）。	真实性	完整性	不可否认性	准确性
2308	单项选择题	根据GM/T 0029《签名验签服务器技术规范》，签名验签服务的消息协议接口采用什么模式（）。	请求响应	输出反馈	UDP模式	后进先出
2309	单项选择题	根据GM/T 0029《签名验签服务器技术规范》，签名验签服务器是用于（）的，为应用实体提供基于PKI体系和数字证书的数字签名、验证签名等运算功能的服务器。	服务端	客户端	终端	前端
2310	单项选择题	根据GM/T 0029《签名验签服务器技术规范》，（）是签名验签服务器的服务对象，可以是个人、机构或系统，其私钥存储在签名验签服务器的密码设备中，能够使用签名验签服务器进行签名及验签运算。	客户	终端	用户	应用实体
2311	单项选择题	根据GM/T 0029《签名验签服务器技术规范》，签名验签服务器的管理界面应具备完善的身份鉴别机制，通过智能密码钥匙、智能IC卡与（）相结合的方式实现管理员身份的鉴别。	密码	口令	函数	数字

2312	单项选择题	根据GM/T 0029《签名验签服务器技术规范》，签名验签服务器应支持通过管理界面导入应用实体的签名证书、加密证书和（ ）。	加密密钥对	签名密钥对	加密密钥	签名密钥
2313	单项选择题	根据GM/T 0029《签名验签服务器技术规范》，以应用程序接口方式提供服务的签名验签服务器，其接口应遵循哪个规范（ ）。	GM/T 0016《智能密码钥匙密码应用接口规范》	GM/T 0017《智能密码钥匙密码应用接口数据格式规范》	GM/T 0018《密码设备应用接口规范》	GM/T 0020《证书应用综合服务接口规范》
2314	多项选择题	根据GM/T 0029《签名验签服务器技术规范》，签名验签服务器的应用管理功能主要包括（ ），并按照安全机制对应用实体的信息进行安全存储。	应用实体的注册	配置密钥	设置私钥授权码	生成管理员
2315	多项选择题	根据GM/T 0029《签名验签服务器技术规范》，应用实体注册的内容可包括（ ）。	设置应用实体名称	配置密钥索引号	导入证书	设置IP地址
2316	多项选择题	根据GM/T 0029《签名验签服务器技术规范》，签名验签服务器应提供日志（ ）功能，具备相应的配置管理和查看界面。	记录	查看	审计	导出
2317	多项选择题	根据GM/T 0029《签名验签服务器技术规范》，签名验签服务器的自检包括密码设备的自检和自身的自检，对（ ）进行检查。在检查不通过时应报警并停止工作。	密码运算功能	随机数发生器	存储的敏感信息	管理功能
2318	多项选择题	根据GM/T 0029《签名验签服务器技术规范》，签名验签服务器的日志内容可以为（ ）。	登录认证	系统配置	密钥管理	应用接口的调用
2319	多项选择题	根据GM/T 0029《签名验签服务器技术规范》，管理员登录成功后，通过管理界面进行（ ）管理操作。	应用管理	证书管理	系统配置	日志查询
2320	多项选择题	根据GM/T 0029《签名验签服务器技术规范》，签名验签服务器应具有对（ ）导入、存储、验证、使用以及备份和恢复等功能。	应用实体证书	用户证书	根证书	证书链

2321	多项选择题	根据GM/T 0029《签名验签服务器技术规范》，签名验签服务器应支持与CA基础设施的连接功能，包括（ ）。	CRL连接配置	OCSP连接配置	RA链接配置	KM链接配置
2322	判断题	根据GM/T 0029《签名验签服务器技术规范》，签名验签服务器应部署在局域网内，只为局域网内的应用实体和用户服务，不能为局域网外的用户使用，不能连接互联网。	正确	错误		
2323	判断题	根据GM/T 0029《签名验签服务器技术规范》，在签名验签服务器注册的应用实体，应由签名验签服务器产生应用实体的加密密钥对和证书请求。	正确	错误		
2324	判断题	根据GM/T 0029《签名验签服务器技术规范》，签名验签服务器应支持CRL连接配置功能，通过配置管理界面，提供从CRL发布点获取CRL、导入CRL等功能。	正确	错误		
2325	判断题	根据GM/T 0029《签名验签服务器技术规范》，签名验签服务器可支持OCSP连接配置功能，通过配置管理界面，进行OCSP服务的连接配置管理。	正确	错误		
2326	判断题	根据GM/T 0029《签名验签服务器技术规范》，应用实体的证书更新时不用保存原来的证书。	正确	错误		
2327	判断题	根据GM/T 0029《签名验签服务器技术规范》，签名验签服务器所使用的操作系统应进行安全加固，裁减一切不需要的模块，关闭所有不需要的端口和服务。	正确	错误		
2328	单项选择题	根据GM/T 0029《签名验签服务器技术规范》，签名验签服务器应用实体必须保存原来自己的（ ），以防止以前的签名不能验证。	公钥	私钥	密钥对	证书

2329	单项选择题	根据GM/T 0029《签名验签服务器技术规范》，签名验签服务器的初始化主要包括（ ）、生成管理员等。使设备处于正常的工作状态。	系统配置	证书导入	密钥导入	日志记录
2330	多项选择题	根据GM/T 0029《签名验签服务器技术规范》，关于签名验签服务器的身份鉴别机制，可以通过（ ）与口令相结合的方式实现身份鉴别。	智能密码钥匙	智能IC卡	口令	证书链
2331	多项选择题	根据GM/T 0029《签名验签服务器技术规范》，签名验签服务器的（ ）等均应由用户方管理人员完成。	系统配置	密钥生成	密钥安装	管理员设置
2332	判断题	根据GM/T 0029《签名验签服务器技术规范》，签名验签服务器不需要设置审计员。	正确	错误		
2333	判断题	根据GM/T 0029《签名验签服务器技术规范》，签名验签服务器能够配置时间源服务器，自动同步时间。	正确	错误		
2334	单项选择题	GM/T 0033《时间戳接口规范》适用范围是（ ）。	基于对称加密算法的产品和应用	基于公钥密码基础设施应用技术体系框架内的时间戳服务相关产品和应用	基于哈希算法的产品和应用	所有密码学相关产品和应用
2335	单项选择题	根据GM/T 0033《时间戳接口规范》，下列选项中是证书机构的缩略语的是（ ）。	CA	TS	GA	RA
2336	单项选择题	根据GM/T 0033《时间戳接口规范》，时间戳机构的英文缩写是（ ）。	TS	TSA	TSP	TSS
2337	单项选择题	根据GM/T 0033《时间戳接口规范》，时间戳请求消息格式包括（ ）。	请求头、请求体	响应头、响应体	请求头、响应头	请求体、响应体
2338	单项选择题	根据GM/T 0033《时间戳接口规范》，时间戳与时间戳系统的通信方式不包含的方式有（ ）。	电子邮件方式	文件方式	socket方式	HTML方式

2339	单项选择题	根据GM/T 0033《时间戳接口规范》，时间戳响应中必须包含有（ ）。	TimeStampReq	TimeStampToken	TimeStampRes	TSTInfo
2340	多项选择题	根据GM/T 0033《时间戳接口规范》，时间戳请求消息体部分包括的字段有（ ）。	请求时间戳算法标识符	请求时间戳信息摘要值	请求证书序列号	请求签名值
2341	多项选择题	在GM/T 0033《时间戳接口规范》中，提及的时间戳响应消息体部分有（ ）。	时间戳信息摘要值	时间戳证书序列号	时间戳签名值	时间戳签名算法标识符
2342	多项选择题	根据GM/T 0033《时间戳接口规范》，STF_GetTSInfo获取时间戳主要信息包括（ ）。	TSA的通用名	时间精度	时间戳标注的时间值	响应方式
2343	判断题	GM/T 0033《时间戳接口规范》中，数字签名可用于确认待签名数据的完整性、签名者身份的真实性和签名行为的抗抵赖性。	正确	错误		
2344	判断题	根据GM/T 0033《时间戳接口规范》，采用文件方式通信时，用户将申请消息存储在一个扩展名为.tsq的文件中传送给TSA，TSA同样将产生的响应消息保存在一个扩展名为.tsr的文件中返回给用户。	正确	错误		
2345	判断题	根据GM/T 0033《时间戳接口规范》，TSA在收到申请消息后，无论申请成功还是失败，都要给请求方返回一个响应消息。	正确	错误		
2346	多项选择题	GM/T 0033《时间戳接口规范》中规定了（ ）。	接口函数	消息格式	传输方式	标识及常量
2347	多项选择题	GM/T 0033《时间戳接口规范》中，时间戳请求被拒绝的原因可能是（ ）。	使用了不支持的算法	非法的申请	可信时间源出现问题	有不理解的附加信息
2348	多项选择题	GM/T 0033《时间戳接口规范》中规定的环境函数包括（ ）。	初始化环境	验证时间戳有效性	获取环境信息	清除环境

2349	多项选择题	GM/T 0033《时间戳接口规范》中，关于时间戳请求消息描述正确的是（ ）。	nonce域是一个随机数	扩展域extension中的非关键扩展无法识别，仍可以生成时间戳	不需要给出请求方的身份标识	certReq域用于验证TSA公钥证书
2350	判断题	GM/T 0033《时间戳接口规范》中，时间戳请求消息的nonce域用于在没有可靠的本地时钟的情况下检验响应消息的合法性并防止重放攻击。	正确	错误		
2351	判断题	GM/T 0033《时间戳接口规范》中，时间戳响应消息无论成功还是失败都将返回一个时间戳响应。	正确	错误		
2352	判断题	GM/T 0033《时间戳接口规范》中，时间戳请求消息应进行双向身份鉴别。	正确	错误		
2353	单项选择题	在GM/T 0123《时间戳服务器密码检测规范》中，初始化操作不包括（ ）	系统配置	初始化管理员或操作员	初始密钥恢复	提供密码服务
2354	单项选择题	在GM/T 0123《时间戳服务器密码检测规范》中，SM2签名算法使用的对象标识符为（ ）	SM2-1数字签名算法 1.2.156.10197.1.301.1	公钥密码算法 1.2.156.10197.1.300	基于SM2算法和SM3算法的签名 1.2.156.10197.1.501	《SM2椭圆曲线公钥密码算法》 1.2.156.10197.6.1.1.3
2355	单项选择题	在GM/T 0123《时间戳服务器密码检测规范》中，SM3杂凑算法使用的对象标识符为	SM3密码杂凑算法，无密钥使用 1.2.156.10197.1.401.1	SM3密码杂凑算法 1.2.156.10197.1.401	基于SM2算法和SM3算法的签名 1.2.156.10197.1.501	《SM3密码杂凑算法》 1.2.156.10197.6.1.1.4
2356	单项选择题	在GM/T 0123《时间戳服务器密码检测规范》中，时间戳服务器应具备（ ）	不少于管理员、审计员、维护员三类角色管理	不少于管理员、审计员两类角色管理	管理员负责设备的日志管理操作	维护员负责设备的维护

2357	单项选择题	在GM/T 0123《时间戳服务器密码检测规范》中，应采用（）的方式登录系统	用户名与登录口令、生物特征相结合	用户名与登录口令、生物特征、智能密码钥匙相结合	智能密码钥匙、智能IC卡等硬件装置与登录口令相结合	智能密码钥匙、智能IC卡等硬件装置与用户名、登录口令相结合
2358	单项选择题	在GM/T 0123《时间戳服务器密码检测规范》中，时间戳服务器（）检测不合格，判定产品不合格	性能检测	设备可靠性检测	设备环境适应性检测	设备安全性检测
2359	多项选择题	在GM/T 0123《时间戳服务器密码检测规范》中，可信时间的源头应来源于（）	国家权威时间部门（如国家授时中心）	使用国家权威时间部门认可的硬件和方法获取的时间	硬件系统时间	CDMA
2360	单项选择题	在GM/T 0123《时间戳服务器密码检测规范》中，时间戳服务器应使用（）进行管理员身份验证	生物特征识别	登录口令	基于数字证书的数字签名	验证码
2361	多项选择题	在GM/T 0123《时间戳服务器密码检测规范》中，以下为密码运算检测项目的是（）	非对称算法检测	对称算法检测	杂凑算法检测	序列算法检测
2362	多项选择题	在GM/T 0123《时间戳服务器密码检测规范》中，要求时间戳服务器至少支持的算法有（）	SM4算法	SM2密码算法	SM3密码算法	SM9密码算法
2363	单项选择题	在GM/T 0123《时间戳服务器密码检测规范》中，要求时间戳服务器应具有的主要部件或接口有（）	电源指示灯	仅1个网络接口	TCM可信计算模块	签名验签服务器
2364	多项选择题	在GM/T 0123《时间戳服务器密码检测规范》中，时间戳服务器宜支持的主要部件或接口有（）	授时天线	串口	冗余电源	手动密钥销毁开关
2365	多项选择题	在GM/T 0123《时间戳服务器密码检测规范》中，设备自检包括（）	上电自检	周期自检	复位自检	接收指令后自检
2366	多项选择题	在GM/T 0123《时间戳服务器密码检测规范》中，时间戳服务器的证书管理和验证功能检测范围包括对应用实体证书、根证书或证书链的（）	导入	使用	备份	验证
2367	多项选择题	在GM/T 0123《时间戳服务器密码检测规范》中，应至少支持用户通过的通信方式包括（）发送时间戳申请	电子邮件	文件	HTTP	SOAP

2368	多项选择题	在GM/T 0123《时间戳服务器密码检测规范》中，可信时间的源头可以来源于（）	通过无线手段获得国家权威时间部门的时间发布	通过长波信号获得国家权威时间部门的时间发布	通过国家权威时间部门认证的原子钟	通过了国家权威时间部门认可的NTP时间源网络地址获得
2369	多项选择题	在GM/T 0123《时间戳服务器密码检测规范》中，时间戳服务器应提供日志（）功能	记录	查看	导出	导入
2370	多项选择题	在GM/T 0123《时间戳服务器密码检测规范》中，时间戳服务器的日志内容应包括（）	管理员操作行为	异常事件	敏感参数	对应用接口的调用进行日志记录
2371	多项选择题	在GM/T 0123《时间戳服务器密码检测规范》中，时间戳服务检测包括（）项目	通信方式	请求和响应格式检测	时间戳接口	可信时间源
2372	判断题	在GM/T 0123《时间戳服务器密码检测规范》中，初始化功能实现设备的初始状态到就绪状态的转换。	正确	错误		
2373	判断题	在GM/T 0123《时间戳服务器密码检测规范》中，应采用经检测认证的具有物理噪声源功能的1个独立芯片，用于实现随机数生成功能。	正确	错误		
2374	判断题	在GM/T 0123《时间戳服务器密码检测规范》中，时间戳签名私钥应在设备外部安全存储。	正确	错误		
2375	判断题	在GM/T 0123《时间戳服务器密码检测规范》中，时间戳签名密钥对的生成应采用经检测认证的2路独立噪声源或密码模块产生	正确	错误		
2376	判断题	在GM/T 0123《时间戳服务器密码检测规范》中，随机数自检应符合GM/T 0062中的E类产品的上电检测和使用检测要求	正确	错误		
2377	判断题	在GM/T 0123《时间戳服务器密码检测规范》中，时间戳服务器的证书管理和验证功能检测时，SM2证书格式应符合GB/T 20518的要求。	正确	错误		

2378	判断题	在GM/T 0123《时间戳服务器密码检测规范》中，时间戳服务器响应的时间格式应是UTC格式。	正确	错误		
2379	判断题	在GM/T 0123《时间戳服务器密码检测规范》中，时间戳服务器使用的签名算法标识应符合GB/T 33560	正确	错误		
2380	判断题	在GM/T 0123《时间戳服务器密码检测规范》中，可信时间的源头可以来源于国家权威时间部门认可的硬件和方法获取的时间	正确	错误		
2381	判断题	在GM/T 0123《时间戳服务器密码检测规范》中，时间戳服务器安全性检测应符合GM/T 0039《密码模块安全检测要求》的规定。	正确	错误		
2382	单项选择题	根据GM/T 0036《采用非接触卡的门禁系统密码应用技术指南》，非接触门禁卡一般包括（）。	射频接口	数字与存储电路	密码模块	以上都有
2383	单项选择题	根据GM/T 0036《采用非接触卡的门禁系统密码应用技术指南》，非接触卡门禁系统中使用的SM4算法是一种（）算法。	分组密码	非对称密码	密码杂凑	流加密
2384	单项选择题	GM/T 0036《采用非接触卡的门禁系统密码应用技术指南》中的应用系统，一般通过各设备内的（）对系统提供密码安全保护。	存储模块	密码模块	通信模块	计算模块
2385	单项选择题	根据GM/T 0036《采用非接触卡的门禁系统密码应用技术指南》，在非接卡门禁系统中下列组件包含密码模块的有（）。	门禁卡	后台管理系统	门禁读卡器	以上都有
2386	单项选择题	根据GM/T 0036《采用非接触卡的门禁系统密码应用技术指南》，关于非接触门禁卡的唯一标识符，下列选项中正确的是（）。	唯一性标识符是由用户写入电子标签芯片的	唯一性标识符是由电子标签芯片制造商固化在电子标签芯片内的。	唯一性标识符就是经注册的厂商代码。	以上都对

2387	单项选择题	关于GM/T 0036《采用非接触卡的门禁系统密码应用技术指南》附录A中，在进行安全模块发行时，后台管理系统使用（ ）中的密码设备生成门禁系统根密钥。	密钥管理子系统	门禁卡	应用系统	门禁读卡器
2388	单项选择题	根据GM/T 0036《采用非接触卡的门禁系统密码应用技术指南》，未使用密码技术的非接触卡主要包含的缺点有（ ）。	容易被复制	容易被篡改	容易泄露敏感数据	以上都有
2389	单项选择题	GM/T 0036《采用非接触卡的门禁系统密码应用技术指南》附录中，采用基于SM1/SM4算法的非接触CPU卡的方案方式与基于SM7算法的非接触式逻辑加密卡所采用的方案类似，主要不同点有（ ）。	安全模块只需支持SM1/SM4算法	门禁卡需要实现一卡一密	门禁卡与非接触读卡器间需要进行身份鉴别	门禁卡与非接触读卡器间需要进行数据加密通讯
2390	单项选择题	根据GM/T 0036《采用非接触卡的门禁系统密码应用技术指南》，RFID的中文是（ ）。	射频识别	射频身份	射频号	射频电路
2391	多项选择题	根据GM/T 0036《采用非接触卡的门禁系统密码应用技术指南》，基于非接触式IC卡的门禁系统的密码应用涉及（ ）。	应用系统	密钥管理及发卡系统	整合系统	学习系统
2392	多项选择题	GM/T 0036《采用非接触卡的门禁系统密码应用技术指南》中的应用系统，一般由（ ）构成。	门禁卡	门禁读卡器	前台管理系统	后台管理系统
2393	多项选择题	根据GM/T 0036《采用非接触卡的门禁系统密码应用技术指南》，发卡子系统的功能是通过发卡设备对门禁卡进行发卡，这些工作包括（ ）。	卡片封装	初始化	注入密钥	写入应用信息
2394	多项选择题	根据GM/T 0036《采用非接触卡的门禁系统密码应用技术指南》，密钥管理及发卡系统包括（ ）。	密钥管理子系统	密钥管理母系统	发卡子系统	发卡母系统
2395	多项选择题	根据GM/T 0036《采用非接触卡的门禁系统密码应用技术指南》，非接触卡门禁系统的要求在密钥（ ）等的整个使用过程中，应保证密钥不被泄漏。	生成	注入	更新	存储

2396	多项选择题	根据GM/T 0036《采用非接触卡的门禁系统密码应用技术指南》，非接触卡门禁系统中，下列组成部分包括射频接口的有（ ）。	门禁卡	后台管理系统	门禁读卡器	数据库
2397	多项选择题	根据GM/T 0036《采用非接触卡的门禁系统密码应用技术指南》，非接触卡门禁系统的密钥管理及发卡系统中的密码设备提供（ ）等密码服务。	密钥生成	密钥分散	对门禁卡发卡时的身份鉴别	初始化
2398	多项选择题	根据GM/T 0036《采用非接触卡的门禁系统密码应用技术指南》，非接触卡门禁系统中应用系统的后台管理系统包括（ ）。	后台管理数据库	密码模块	前台管理数据库	射频接口
2399	判断题	根据GM/T 0036《采用非接触卡的门禁系统密码应用技术指南》，门禁卡内的密码模块主要用于门禁读卡器或后台管理系统对门禁卡进行身份鉴别时提供密码服务。	正确	错误		
2400	判断题	根据GM/T 0036《采用非接触卡的门禁系统密码应用技术指南》，在门禁系统的具体方案设计时，必须在门禁读卡器和后台管理系统内都配用密码模块。	正确	错误		
2401	判断题	根据GM/T 0036《采用非接触卡的门禁系统密码应用技术指南》，非接触卡门禁系统所使用的密钥，在密钥生成过程中不需要使用随机数，生成过程可以预测。	正确	错误		
2402	判断题	根据GM/T 0036《采用非接触卡的门禁系统密码应用技术指南》，门禁系统的根密钥是由门禁卡的安全模块生成的。	正确	错误		
2403	判断题	根据GM/T 0036《采用非接触卡的门禁系统密码应用技术指南》，门禁卡可以用来对系统根密钥进行密钥分散。	正确	错误		

2404	判断题	GM/T 0036《采用非接触卡的门禁系统密码应用技术指南》附录A中提到的基于SM7算法的非接触式逻辑加密卡方案中，在执行门禁卡发卡时，是通过发卡读写器对卡片进行数据结构的初始化、卡片密钥的下载、发行信息的写入等操作的。	正确	错误		
2405	单项选择题	GM/T 0036《采用非接触卡的门禁系统密码应用技术指南》，门禁卡需要实现（ ）。	一卡一密	一次一密	一次三密	一次多密
2406	单项选择题	GM/T 0036《采用非接触卡的门禁系统密码应用技术指南》，可以使用（ ）算法。	DES	AES	SM4	3DES
2407	多项选择题	GM/T 0036《采用非接触卡的门禁系统密码应用技术指南》，门禁系统的应用系统一般由如下哪些部分构成（ ）。	门禁卡	读卡器	后台管理系统	保险柜
2408	多项选择题	在GM/T 0036《采用非接触卡的门禁系统密码应用技术指南》中，密钥管理与发卡系统的功能包括（ ）。	生成密钥	注入密钥	刷卡开门	密钥分散
2409	多项选择题	GM/T 0036《采用非接触卡的门禁系统密码应用技术指南》，可使用的算法有（ ）。	SM4	SM1	DES	SM7
2410	判断题	GM/T 0036《采用非接触卡的门禁系统密码应用技术指南》指导的是接触卡门禁管理。	正确	错误		
2411	判断题	GM/T 0036《采用非接触卡的门禁系统密码应用技术指南》，算法可以随便使用。	正确	错误		
2412	判断题	GM/T 0036《采用非接触卡的门禁系统密码应用技术指南》是一个检测规范。	正确	错误		
2413	单项选择题	GM/T 0036《采用非接触卡的门禁系统密码应用技术指南》。门禁系统鉴别协议遵循（ ）。	GM/T 0032	GM/T 0033	GM/T 0034	GM/T 0035

2414	多项选择题	GM/T 0021《动态口令密码应用技术规范》动态口令生成算法使用了（ ）国密算法。	SM1	SM2	SM3	SM4
2415	单项选择题	根据GM/T 0021《动态口令密码应用技术规范》，动态口令生成方式中，种子密钥的长度应不少于（ ）比特。	8	32	64	128
2416	单项选择题	根据GM/T 0021《动态口令密码应用技术规范》，动态口令生成方式中，口令变化周期的最大长度应为（ ）秒。	30	60	90	120
2417	单项选择题	根据GM/T 0021《动态口令密码应用技术规范》，关于动态令牌的安全特性，以下描述中不正确的是（ ）。	令牌必须拥有种子密钥的保护功能	令牌完成种子密钥导入后，通讯I/O端口应失效，不能再输入或输出信息	具有数字和功能按键的令牌应具有PIN防暴力穷举功能	种子密钥可通过动态令牌芯片的调试接口读出
2418	单项选择题	GM/T 0021《动态口令密码应用技术规范》中的令牌同步过程，对于时间型令牌应使用（ ）方式。	双向时间窗口	单向时间窗口	双向事件窗口	单向事件窗口
2419	单项选择题	根据GM/T 0021《动态口令密码应用技术规范》，令牌同步过程中，对于事件型令牌应使用（ ）方式。	双向时间窗口	单向时间窗口	双向事件窗口	单向事件窗口
2420	单项选择题	GM/T 0021《动态口令密码应用技术规范》中要求，PIN输入错误的次数如果超过5次，应至少等待（ ）才可继续尝试。	1分钟	5分钟	1小时	24小时
2421	单项选择题	根据GM/T 0021《动态口令密码应用技术规范》，激活时需要验证动态口令，应使用（ ）。	大窗口	中窗口	小窗口	大小不超过±2 的窗口
2422	单项选择题	GM/T 0021《动态口令密码应用技术规范》中，（ ）工作状态的动态令牌可用于口令认证。	未激活	就绪	锁定	作废
2423	单项选择题	根据GM/T 0021《动态口令密码应用技术规范》，关于动态口令系统的各个组成部分，以下说法不正确的是（ ）。	动态令牌负责生成动态口令	认证系统负责验证动态口令的正确性	密钥管理系统负责密钥管理	应用系统负责负责验证动态口令的正确性

2424	多项选择题	GM/T 0021《动态口令密码应用技术规范》规定，种子密钥的安全性应该从哪（）方面进行保护。	种子密钥生成	种子密钥传输	种子密钥存储	种子密钥使用
2425	多项选择题	根据GM/T 0021《动态口令密码应用技术规范》，动态口令系统中的密钥管理系统，涉及的密钥除了种子密钥和主密钥之外，还包括的密钥有（）。	厂商生产主密钥	种子密钥加密密钥	传输密钥	厂商种子密钥加密密钥
2426	多项选择题	根据GM/T 0021《动态口令密码应用技术规范》，密钥管理安全设计应遵循的原则有（）。	采用国家密码管理局批准的硬件密码设备	主密钥的生成由专用硬件生成	主密钥的存储由专用硬件存储且可导出	所有密钥的运算都在专用硬件中完成
2427	多项选择题	根据GM/T 0021《动态口令密码应用技术规范》，关于令牌物理安全描述正确的是（）。	令牌应防范通过物理攻击的手段获取设备内的敏感信息	令牌芯片的令牌掉电后，种子密钥无需自动销毁	令牌芯片应保护种子密钥无法通过外部或内部的方式读出	令牌完成种子密钥导入后，通讯I/O端口应失效，不能再输入或输出信息
2428	多项选择题	根据GM/T 0021《动态口令密码应用技术规范》，根据GM/T 0021《动态口令密码应用技术规范》，时间型令牌使用窗口同步，以下对窗口及其大小描述正确的是（）。	大窗口，窗口大小不应超过±30	大窗口，窗口大小不应超过±10	中窗口，窗口大小不应超过±5	小窗口，窗口大小不应超过±2
2429	多项选择题	根据GM/T 0021《动态口令密码应用技术规范》，根据GM/T 0021《动态口令密码应用技术规范》，认证系统安全服务包含（）。	动态口令认证	令牌生命周期管理	挑战应答认证	挑战码生成
2430	多项选择题	根据GM/T 0021《动态口令密码应用技术规范》，动态口令生成方法中，参与运算的动态因子包括的类型有（）。	时间因子	事件因子	挑战因子	生物特征
2431	多项选择题	根据GM/T 0021《动态口令密码应用技术规范》，属于令牌生命周期管理的内容有（）。	激活	锁定	挂起	作废

2432	多项选择题	根据GM/T 0021《动态口令密码应用技术规范》，除了系统登录认证、用户管理、种子密钥管理、令牌生产配置和时间同步之外，动态口令系统中的密钥管理系统还应至少具备的功能包括（）。	产生挑战码	保护密钥管理	令牌序列号管理	动态口令认证
2433	判断题	根据GM/T 0021《动态口令密码应用技术规范》，令牌内的种子密钥不能被导出产品外部。	正确	错误		
2434	判断题	根据GM/T 0021《动态口令密码应用技术规范》，自动解锁只能解除被自动锁定的令牌。	正确	错误		
2435	判断题	根据GM/T 0021《动态口令密码应用技术规范》，只有就绪或锁定状态的令牌可以被设置为挂起状态。	正确	错误		
2436	判断题	根据GM/T 0021《动态口令密码应用技术规范》，生成的挑战码的格式必须为数字+字符型。	正确	错误		
2437	判断题	根据GM/T 0021《动态口令密码应用技术规范》，挑战码的最小长度和最大长度不能由认证系统进行设置。	正确	错误		
2438	判断题	根据GM/T 0021《动态口令密码应用技术规范》，令牌损坏或失效后，可通过认证系统将其废止。	正确	错误		
2439	判断题	根据GM/T 0021《动态口令密码应用技术规范》，动态口令的基本认证原理，是通过用户端与认证服务提供端，以相同的运算因子，采用相同的运算方法，生成相同的口令，并进行比对，来完成整个认证过程。	正确	错误		
2440	单项选择题	在GM/T 0021《动态口令密码应用技术规范》中，关于动态口令生成方式中的N的最小长度应为（）。	4	6	10	16
2441	单项选择题	GM/T 0021《动态口令密码应用技术规范》中规定，一个动态口令的最大有效时限是（）。	10秒	30秒	60秒	120秒

2442	多项选择题	GM/T 0021《动态口令密码应用技术规范》动态口令的生成使用到的有（）。	算法函数	截位函数	数据组装	求余运算
2443	多项选择题	GM/T 0021《动态口令密码应用技术规范》动态口令系统中动态令牌负责（）动态口令。	产生	显示	比对	验证
2444	判断题	GM/T 0021《动态口令密码应用技术规范》动态口令是身份鉴别的唯一算法。	正确	错误		
2445	判断题	GM/T 0021《动态口令密码应用技术规范》动态口令系统中密钥管理系统负责种子密钥的生成、传输。	正确	错误		
2446	判断题	GM/T 0021《动态口令密码应用技术规范》使用SM3算法产生的动态口令比使用SM4算法产生的动态口令长。	正确	错误		
2447	多项选择题	GM/T 0021《动态口令密码应用技术规范》对提交的动态口令进行认证的认证方式包括（ ）。	静态口令	动态口令	动态口令+静态口令	免口令
2448	单项选择题	GM/T 0031《安全电子签章密码技术规范》中的规定范围是（）。	电子印章和电子签章的数据结构、密码处理流程	电子印章数据结构	电子签章数据结构	电子签章密码处理流程
2449	单项选择题	GM/T 0031《安全电子签章密码技术规范》中对制章人的描述正确的是（）。	制章人只能是单位证书	制章人是电子印章系统中对文档进行签章操作的最终用户	制章人即电子印章系统中具有签署和管理电子印章信息权限的管理员	电子印章数据结构包括制章人信息即可，可以不包含制章人签名信息
2450	单项选择题	GM/T 0031《安全电子签章密码技术规范》中定义安全电子印章数据格式的作用,下列描述错误的是（）。	确保电子印章的完整性	确保电子印章的不可伪造性	确保只有合法用户才能使用	确保文档的机密性
2451	单项选择题	GM/T 0031《安全电子签章密码技术规范》中电子印章数据中的“印章信息”结构不包括（）。	头信息	签名信息	印章标识	印章图片信息

2452	单项选择题	GM/T 0031《安全电子签章密码技术规范》中电子印章数据中的“印章签名信息”不包括（）。	制章人证书	签名算法标识	签名值	签章人证书
2453	单项选择题	GM/T 0031《安全电子签章密码技术规范》中电子签章数据格式组装待签名数据表述最全面的是（）。	版本号、电子印章、时间信息、原文杂凑值、原文属性信息、签章人证书、签名算法标识	原文杂凑值	签章人证书	签名算法标识
2454	单项选择题	GM/T 0031《安全电子签章密码技术规范》电子“印章信息”的结构不包括（）。	头信息	电子印章标识	自定义数据	签章人证书杂凑值
2455	单项选择题	GM/T 0031《安全电子签章密码技术规范》不属于电子印章数据格式中属性信息的是（）。	印章制作日期	印章有效终止日期	电子印章标识	印章有效期起始日期
2456	单项选择题	GM/T 0031《安全电子签章密码技术规范》电子印章数据格式中签名信息结构中的证书是（）。	签章人证书	制章人证书	管理员证书	单位证书
2457	单项选择题	GM/T 0031《安全电子签章密码技术规范》规定，如果签章人证书执行更新、重签发等操作导致证书对比失败，应该执行（）。	比对证书CN项，一致则验证通过	比对证书DN项，一致则验证通过	重新制作印章	验证通过
2458	单项选择题	GM/T 0031《安全电子签章密码技术规范》中原文数据的属性信息是否可以自定义，下列描述正确的是（）。	不可以，属性信息必须是整个文档	可以	不可以，属性信息必须是签章保护范围	不可以，属性信息必须是文档ID
2459	单项选择题	GM/T 0031《安全电子签章密码技术规范》中不属于印章图片类型的是（）。	GIF	BMP	JPG	XML
2460	多项选择题	GM/T 0031《安全电子签章密码技术规范》电子印章数据的结构包括（）。	印章信息	签名信息	签章信息	原文属性
2461	多项选择题	GM/T 0031《安全电子签章密码技术规范》电子印章头信息包含的信息有（）。	厂商ID	标识	版本号	有效期

2462	多项选择题	GM/T 0031《安全电子签章密码技术规范》电子印章图片信息包含（ ）。	图片类型	图片数据	图片显示的宽度和高度	图片标题
2463	多项选择题	GM/T 0031《安全电子签章密码技术规范》属于电子签章验证环节的是（ ）。	验证电子签章数据格式的合规性	验证电子签章签名值是否正确	验证签章人数字证书有效性	验证原文杂凑
2464	多项选择题	GM/T 0031《安全电子签章密码技术规范》中规定（ ）原因导致的签章人证书有效性验证失败，可直接退出验证流程。	证书有效期过期错误	密钥用法不正确	证书信任链验证失败	证书状态已吊销
2465	多项选择题	GM/T 0031《安全电子签章密码技术规范》中规定验证制章人证书的有效性，验证项至少包括（ ）。	制章人证书信任链验证	制章人证书有效期验证	制章人证书撤销时间	密钥用法是否正确
2466	多项选择题	GM/T 0031《安全电子签章密码技术规范》中电子印章的有效期验证需要获取印章格式的（ ）信息。	印章有效起始日期	印章有效终止日期	制章人证书有效期	制章日期
2467	多项选择题	GM/T 0031《安全电子签章密码技术规范》中验证签章的时间有效性中规定下列视为签章无效的情况包括（ ）。	签章时间不在签章人数字证书有效期内	签章时间处于签章人数字证书有效期内，并且证书有效	签章时间处于签章人数字证书有效期内，但是证书在签章之前已被吊销	签章时间处于签章人数字证书有效期内，但是证书在签章之后被吊销
2468	判断题	GM/T 0031《安全电子签章密码技术规范》电子签章结构中包含电子印章结构。	正确	错误		
2469	判断题	GM/T 0031《安全电子签章密码技术规范》电子印章标识是电子印章数据的唯一标识编码。	正确	错误		
2470	判断题	GM/T 0031《安全电子签章密码技术规范》规定电子签章数据由版本号、电子印章、时间信息、原文杂凑值、原文属性信息、证书标识、签名算法标识及签名值等组成。	正确	错误		
2471	判断题	GM/T 0031《安全电子签章密码技术规范》规定电子印章头信息中的电子印章数据标识固定为"ES"	正确	错误		

2472	判断题	GM/T 0031《安全电子签章密码技术规范》中定义的电子印章和电子签章格式相同。	正确	错误		
2473	单项选择题	GM/T 0031-2014《安全电子签章密码技术规范》电子印章数据结构中的签名信息字段是（ ）。	签章人的数字签名	制章人的数字签名	印章持有者的数字签名	用户的数字签名
2474	单项选择题	GM/T 0031-2014《安全电子签章密码技术规范》电子签章数据结构中的签名值是（ ）。	制章人的数字签名	用户的数字签名	签章人的数字签名	编写人的数字签名
2475	单项选择题	GM/T 0031-2014《安全电子签章密码技术规范》电子签章中的时间信息字段是（ ）。	印章的制作时间	印章的有效起始日期	印章的终止起始日期	电子签章产生的时间
2476	单项选择题	GM/T 0031-2014《安全电子签章密码技术规范》电子印章是通过（ ）来将签章人身份与签章图片进行绑定。	授权管理	加密	数字签名	访问控制
2477	多项选择题	GM/T 0031-2014《安全电子签章密码技术规范》通过使用安全电子签章技术，可以确保文档的（ ）。	机密性	完整性	来源的真实性	不可否认性
2478	多项选择题	GM/T 0031-2014《安全电子签章密码技术规范》主要规范了（ ）的数据结构、密码处理流程。	电子印章	电子签名	电子签章	时间戳
2479	多项选择题	GM/T 0031-2014《安全电子签章密码技术规范》电子印章中的签名范围包括（ ）。	印章信息	制章人数字证书	签名算法标识	待签章原文属性信息
2480	单项选择题	GM/T 0031-2014《安全电子签章密码技术规范》电子印章中的签名范围不包括（ ）	印章信息	制章人数字证书	签名算法标识	待签章原文属性信息
2481	判断题	GM/T 0031-2014《安全电子签章密码技术规范》电子印章的安全性是通过签章人的数字签名保护的。	正确	错误		
2482	单项选择题	GM/T 0047《安全电子签章密码检测规范》规定的电子印章数据中的数据内容和编码需满足以下（ ）协议的要求。	GM/T 0031-2014安全电子签章密码技术规范	GM/T 0014《数字证书认证系统密码协议规范》	GM/T 0012《可信计算可信密码模块接口规范》	GM/T 0029《签名验签服务器技术规范》

2483	单项选择题	根据GM/T 0047《安全电子签章密码检测规范》，缩略语PKCS指的是（）。	公钥基础设施	数字信封	公钥密码标准	扩展证书内容
2484	单项选择题	GM/T 0047《安全电子签章密码检测规范》中电子印章的验证不包括（）。	印章签名值验证	制章人证书有效性验证	签章人证书有效性验证	印章有效期验证
2485	单项选择题	GM/T 0047《安全电子签章密码检测规范》中电子签章验证不包括（）。	电子签章签名值验证	消息鉴别码验证	签章人证书有效性验证	签章中电子印章有效性验证
2486	单项选择题	GM/T 0047《安全电子签章密码检测规范》中电子签章签名值验证，下列不属于待验证数据的是（）。	版本号	时间信息	原文杂凑值	时间戳
2487	单项选择题	GM/T 0047《安全电子签章密码检测规范》规定签章人证书有效性验证中，验证项不包括（）。	制章人证书扩展项	签章人证书有效期验证	签章人证书是否被吊销	签章人证书密钥用法是否正确
2488	单项选择题	GM/T 0047《安全电子签章密码检测规范》规定的电子签章验证检测中，关于签章时间有效期验证检测，以下判断规则错误的是（）。	如果签章时间处于签章人数字证书有效期内，并且证书有效，则签章时间有效	如果签章时间不在签章人数字证书有效期内，则签章时间无效	如果签章时间处于签章人数字证书有效期内，但是证书在签章之前已被吊销，则签章时间有效	如果签章时间处于签章人数字证书有效期内，但是证书在签章之后被吊销，则签章时间有效
2489	单项选择题	GM/T 0047《安全电子签章密码检测规范》规定的电子印章验证检测中，印章签名值验证检测中，以下判断规则错误的是（）。	输入签名值错误的电子印章数据，然后使用电子印章系统进行验证，如果验证失败，则测试通过；否则测试失败	更改正确电子印章数据的签名原文，然后使用电子印章系统进行验证，如果验证通过，则测试通过；否则，测试失败	更改正确电子印章数据的签名原文，然后使用电子印章系统进行验证，如果验证失败，则测试通过；否则，测试失败	输入正确的电子印章数据，然后使用电子印章系统进行验证，如果验证通过，则测试通过;否则，测试失败

2490	单项选择题	GM/T 0047《安全电子签章密码检测规范》规定的签章人证书有效性验证检测，以下判断规则错误的是（ ）。	电子印章系统使用正确的证书信任链，验证在有效期内、未吊销、密钥用法正确的签章人证书，如果验证通过，则本步测试通过；否则，测试失败	电子印章系统使用错误的证书信任链，验证签章人证书，如果验证失败，则本步测试通过；否则，测试失败	电子印章系统验证处于非电子印章有效期内的签章人证书，如果验证通过，则本步测试通过；否则，测试失败	电子印章系统验证吊销时间在签章时间之前的签章人证书，如果验证失败，则本步测试通过；否则，测试失败
2491	单项选择题	GM/T 0047《安全电子签章密码检测规范》规定的签章原文杂凑验证检测，下列判断规则不正确的是（ ）。	输入正确的电子签章及对应的签章原文，使用电子印章系统验证签章原文杂凑值，如果验证通 过,则本步测试通过,否则，测试失败	输入正确的电子签章及修改后的签章原文，使用电子印章系统验证签章原文杂凑值，如果验证失败,则本步测试通过,否则，测试失败	输入修改了杂凑值的电子签章及对应的签章原文，使用电子印章系统验证签章原文杂凑值，如果验证失败，则本步测试通过，否则，测试失败	输入正确的电子签章及修改后的签章原文，使用电子印章系统验证签章原文杂凑值，如果验证通过,则本步测试通过,否则，测试失败
2492	单项选择题	GM/T 0047《安全电子签章密码检测规范》中验证电子签章时导致验证失败的原因不包括（ ）。	原文杂凑值改变	签章时间不在电子印章有效期内	电子印章系统使用制章时间处于制章人证书有效期之外的电子印章	签章人证书的吊销时间在签章时间之后。
2493	多项选择题	GM/T 0047《安全电子签章密码检测规范》中电子印章验证包括（ ）。	印章数据格式验证	印章签名值验证	制章人证书有效性验证	印章有效期验证
2494	多项选择题	GM/T 0047《安全电子签章密码检测规范》规定的电子印章验证检测中，根据（ ）验证电子印章签名信息中的签名值的准确性。	印章信息数据	制章人证书	签章人证书	签名算法标识

2495	多项选择题	GM/T 0047《安全电子签章密码检测规范》规定的电子印章验证检测中，制章人证书有效性验证，属于验证项的有（ ）。	制章人证书信任链验证	制章人证书有效期验证	制章人证书是否被吊销	密钥用法是否正确
2496	多项选择题	GM/T 0047《安全电子签章密码检测规范》规定的电子签章验证包括（ ）。	电子签章数据格式验证	电子签章签名值验证	签章人证书有效性验证	签章原文杂凑验证
2497	多项选择题	GM/T 0047《安全电子签章密码检测规范》规定的电子签章签名值验证功能中，待验证数据包括（ ）。	电子印章	原文杂凑值	签名算法标识	原文属性信息
2498	多项选择题	GM/T 0047《安全电子签章密码检测规范》规定的签章时间有效期验证检测，下列判断规则正确的是（ ）。	如果签章时间处于签章人数字证书有效期内，并且证书有效，则签章时间有效	如果签章时间不在签章人数字证书有效期内，则签章时间无效	如果签章时间处于签章人数字证书有效期内，但是证书在签章之前已被吊销，则签章时间无效	如果签章时间处于签章人数字证书有效期内，但是证书在签章之后被吊销，则签章时间有效
2499	多项选择题	GM/T 0047《安全电子签章密码检测规范》规定的电子签章数据格式验证检测中，下列判断规则正确的是（ ）。	输入正确数据格式的电子签章数据，然后使用电子印章系统进行验证，如果验证通过，则本步 测试通过；否则，测试失败	输入正确数据格式的电子签章数据，然后使用电子印章系统进行验证，如果验证失败，则本步 测试通过；否则，测试失败	输入错误数据格式的电子签章数据，然后使用电子印章系统进行验证，如果验证失败，则本步 测试通过；否则，测试失败	输入错误数据格式的电子签章数据，然后使用电子印章系统进行验证，如果验证通过，则本步 测试通过；否则，测试失败
2500	多项选择题	GM/T 0047《安全电子签章密码检测规范》规定的电子签章签名值验证检测中，下列判断规则正确的是	输入签名值正确的电子签章数据，然后使用电子印章系统进行验证，如果验证通过，则本步测试通过；否则，测试失败。	输入签名值正确的电子签章数据，然后使用电子印章系统进行验证，如果验证失败，则本步测 试通过；否则，测试失败。	输入签名值错误的电子签章数据，然后使用电子印章系统进行验证，如果验证通过，则本步测试通过；否则，测试失败。	输入签名值错误的电子签章数据，然后使用电子印章系统进行验证，如果验证失败，则本步测 试通过；否则，测试失败。

2501	多项选择题	GM/T 0047《安全电子签章密码检测规范》规定的电子印章有效性验证，下列判断规则正确的是（）。	输入签章时间处于电子印章有效期内的电子签章，使用电子印章系统进行有效性验证,如果测试通过，则本步测试通过;否则，测试失败	输入签章时间处于非电子印章有效期内的电子签章,使用电子印章系统进行有效性验证，如果测试不通过，则本步测试通过；否则，测试失败	输入签章时间处于非电子印章有效期内的电子签章,使用电子印章系统进行有效性验证，如果测试通过，则本步测试通过；否则，测试失败	输入签章时间处于电子印章有效期内的电子签章，使用电子印章系统进行有效性验证,如果测试不通过，则本步测试通过;否则，测试失败
2502	判断题	GM/T 0047《安全电子签章密码检测规范》规定的电子签章数据检测中，需要电子签章数据的数据内容和编码格式都正确，对密码算法无要求。	正确	错误		
2503	判断题	GM/T 0047《安全电子签章密码检测规范》规定的电子印章是一种由制作者签名的包括持有者信息和图形化内容的数据，可用于签署电子文件。	正确	错误		
2504	判断题	GM/T 0047《安全电子签章密码检测规范》规定的制章人是电子印章系统中具有签署和管理电子印章信息权限的管理员,管理员的数字证书只能是单位证书。	正确	错误		
2505	判断题	GM/T 0047《安全电子签章密码检测规范》中规定，在验证电子签章有效性时，签章时间有效性与电子印章有效期无关。	正确	错误		
2506	判断题	GM/T 0047《安全电子签章密码检测规范》规定的验证电子签章有效性时，如果电子签章中的签章时间信息处于签章人证书有效期之外，则应验证失败。	正确	错误		

2507	判断题	GM/T 0047《安全电子签章密码检测规范》规定的如果签章时间处于签章人数字证书有效期内，但是证书在签章之后被吊销，则签章时间无效。	正确	错误		
2508	判断题	GM/T 0047《安全电子签章密码检测规范》规定的电子印章系统应提供电子签章原文杂凑验证功能，如果签章原文改变或电子签章数据中的原文杂凑值改变，都会导致验证失败。	正确	错误		
2509	单项选择题	GM/T 0047《安全电子签章密码检测规范》电子印章签名值验证，要使用（ ）验证签名。	签章人证书	持章人证书	制章人证书	法人证书
2510	单项选择题	GM/T 0047《安全电子签章密码检测规范》签章原文杂凑验证检测步骤，不包含的操作是（ ）。	用正确的签章原文去验证	用修改后的签章原文去验证	用修改了杂凑值的电子签章原文去验证	验证签章者证书
2511	单项选择题	GM/T 0047《安全电子签章密码检测规范》通过使用安全电子签章技术，不能确保文档的（ ）。	机密性	完整性	来源的真实性	不可否认性
2512	单项选择题	GM/T 0047《安全电子签章密码检测规范》规范了（ ）的密码检测内容、检测要求、检测方法，以及合格判定准则。	电子印模	电子签名	电子签章	时间戳
2513	多项选择题	GM/T 0047《安全电子签章密码检测规范》签章人证书有效性验证包括（ ）。	证书信任链	证书有效期	证书处于未吊销状态	密钥用法
2514	判断题	GM/T 0047《安全电子签章密码检测规范》电子签章是指使用电子印章签署电子文件的过程。	正确	错误		
2515	判断题	GM/T 0047《安全电子签章密码检测规范》电子签章结构中包含原文数据本身。	正确	错误		
2516	判断题	GM/T 0047《安全电子签章密码检测规范》电子签章验证检测过程不包含电子印章有效性进行检测。	正确	错误		

2517	多项选择题	GM/T 0031《安全电子签章密码技术规范》电子印章中一般包含哪些原文信息（ ）。	原文内容本身	原文杂凑	原文属性信息	原文名称
2518	单项选择题	GM/T 0055《电子文件密码应用技术规范》规定的关于安全电子文件的标签长度叙述正确的是（）。	安全电子文件的标签长度是定长的	安全电子文件的标签长度是不定长的	安全电子文件的标签长度是定长或不定长	与文件大小有关
2519	单项选择题	GM/T 0055《电子文件密码应用技术规范》规定的安全电子文件的标签数据格式编码规则是（）。	BASE64	UTF8	ASCII	ASN.1
2520	单项选择题	GM/T 0055《电子文件密码应用技术规范》规定的安全电子文件的标签存储形式为（）。	安全电子文件的标签存储形式仅可采用内联式	安全电子文件的标签存储形式仅可采用外联式	安全电子文件的标签存储形式可采用内联式和外联式	安全电子文件的标签存储形式内存式和文件式
2521	单项选择题	GM/T 0055《电子文件密码应用技术规范》规定的标签格式，按外联式存储，则标签和文件存放于两个独立的物理文件，其标签和文件实体之间的对应关系的管理者是（）。	标签	安全电子文件密码服务中间件	密码设备	安全电子文件应用系统
2522	单项选择题	GM/T 0055《电子文件密码应用技术规范》规定标签与文件绑定关系的建立与验证的提供者是（）。	标签	安全电子文件密码服务中间件	密码设备	应用系统
2523	单项选择题	GM/T 0055《电子文件密码应用技术规范》规定使用公钥密码算法的密钥对有（）。	加密密钥对	签名密钥对	加密密钥对或签名密钥对	加密密钥对和签名密钥对
2524	单项选择题	GM/T 0055《电子文件密码应用技术规范》规定标签头中的签名值计算内容叙述正确的是（）。	标签的所有内容	标签体的所有内容	除标签头签名以外的所有标签内容	除签名以外的所有标签内容
2525	单项选择题	GM/T 0055《电子文件密码应用技术规范》规定文件和标签内容采用的加密算法类型为（）。	对称算法	非对称算法	杂凑算法	都可以
2526	单项选择题	GM/T 0055《电子文件密码应用技术规范》规定对称算法使用的密码工作模式为 OFB 和 CFB 时，应用的反馈位数由（）设置。	安全电子文件密码服务中间件	密码设备	应用系统	以上都可以

2527	单项选择题	GM/T 0055《电子文件密码应用技术规范》规定对文件和标签内容进行加密时，其加密数据的填充方式遵循（ ）。	PKCS#1	PKCS#5	PKCS#7	以上都可以
2528	单项选择题	GM/T 0055《电子文件密码应用技术规范》规定签名及验证和数字信封操作使用公钥算法，当使用SM2算法时，格式应遵循（ ）。	PKCS#1	PKCS#5	PKCS#7	GM/T 0009《SM2 密码算法使用规范》
2529	多项选择题	GM/T 0055《电子文件密码应用技术规范》中提出基于标签的安全电子文件系统组成部分主要有（ ）。	应用系统	安全电子文件密码服务中间件	基础密码服务	个性密码服务
2530	单项选择题	关于GM/T 0055《电子文件密码应用技术规范》，下列关于安全电子文件的叙述不正确的是（ ）。	安全电子文件存储形式支持内联式和外联式	标签是安全电子文件的组成部分	标签只能由中间件进行处理	标签通过用户身份标识与实体文件进行唯一绑定
2531	多项选择题	GM/T 0055《电子文件密码应用技术规范》关于标签与文件实体的相关叙述正确的是（ ）。	标签头可加密	标签体可加密	标签可加密	文件实体可加密
2532	多项选择题	GM/T 0055《电子文件密码应用技术规范》规定当应用系统对中间件发出操作请求，中间件响应处理，下列哪些过程是属于中间件的处理过程（ ）。	获取操作者身份、标签和文件	验证文件和标签进行绑定关系	判定操作权限的合法性	调用密码服务
2533	多项选择题	GM/T 0055《电子文件密码应用技术规范》关于标签安全保护体系相关叙述正确的是（ ）。	标签体存放保护文件的相关属性	标签头存放标签体的相关属性	标签应加密保护	标签应签名保护
2534	多项选择题	GM/T 0055《电子文件密码应用技术规范》规定的安全电子文件，通过标签与文件建立唯一绑定关系，下列关于验证标签与文件绑定关系的流程叙述哪些是正确的（ ）。	除标签头中的签名值属性外的所有标签内容计算摘要	验证标签签名	文件内容计算摘要	验证文件签名
2535	多项选择题	GM/T 0055《电子文件密码应用技术规范》规定对称算法采用的加密模式有（ ）。	ECB	CBC	OFB	CFB
2536	多项选择题	GM/T 0055《电子文件密码应用技术规范》规定标签体属性结构定义，下列属于标签体里的属性的有（ ）。	标识属性	扩展属性	权限属性	日志属性

2537	多项选择题	GM/T 0055《电子文件密码应用技术规范》规定文件签名是指对应用系统提交的文件进行签名操作，下列叙述正确的是（ ）。	获取签名算法标识	使用算法标识中指定的杂凑算法对文件计算摘要	使用操作者签名私钥对摘要值进行数字签名	签名属性内容置于标签体的签名属性集合
2538	判断题	GM/T 0055《电子文件密码应用技术规范》其定义的标签数据格式包括扩展属性，但其作为保留属性，用于应用系统定义自身的各种属性。	正确	错误		
2539	判断题	GM/T 0055《电子文件密码应用技术规范》规定标签中的标签体可加密，也可以不加密。	正确	错误		
2540	判断题	GM/T 0055《电子文件密码应用技术规范》规定中间件为应用系统提供服务是按请求/响应形式提供的。	正确	错误		
2541	判断题	GM/T 0055《电子文件密码应用技术规范》规定标签的存储形式有内联式和外联式两种形式。	正确	错误		
2542	判断题	GM/T 0055《电子文件密码应用技术规范》规定内联式标签存储形式是一个物理文件，外联式标签存储形式可以是一个物理文件也可以是两个物理文件。	正确	错误		
2543	判断题	GM/T 0055《电子文件密码应用技术规范》规定中间件的密码机制基于 PKI 体制，使用数字证书机制对文件进行安全保护，数字证书应使用双数字证书。	正确	错误		
2544	判断题	GM/T 0055《电子文件密码应用技术规范》规定安全电子文件的标识固定为“@SFL”。	正确	错误		
2545	判断题	GM/T 0055《电子文件密码应用技术规范》规定电子文件签名的形式可支持多用户逐次签名。	正确	错误		
2546	多项选择题	GM/T 0055《电子文件密码应用技术规范》中提出个性密码服务，下列属于个性密码服务的有（ ）。	电子印章	数字水印	指纹	智能密码钥匙

2547	单项选择题	GM/T 0055《电子文件密码应用技术规范》规定标签头属性结构定义，下列不属于标签头里的属性是（ ）。	自定义属性	日志属性	加密属性	签名属性
2548	单项选择题	GM/T 0055《电子文件密码应用技术规范》对实体文件进行数据加密的算法是（ ）。	对称算法	非对称算法	杂凑算法	都可以
2549	单项选择题	下列关于GM/T 0055《电子文件密码应用技术规范》的相关叙述不正确的是（ ）。	标签是电子文件密码服务中间件的操作对象	文件是电子文件密码服务中间件的操作对象	标签与文件存在唯一绑定关系	标签分别存放在外联式存储的两个独立文件中
2550	单项选择题	根据GM/T 0071《电子文件密码应用指南》，电子文件全生命周期中经历的三种类型的系统不包括的系统有（ ）。	文件审批系统	业务系统	电子文件管理系统	电子文件长期保存系统
2551	单项选择题	根据GM/T 0071《电子文件密码应用指南》，电子文件的密码操作使用的算法不包括（ ）。	杂凑算法	对称算法	共识算法	非对称算法
2552	单项选择题	根据GM/T 0071《电子文件密码应用指南》，在电子文件应用参考中，电子文件接收办理不包括的环节有（ ）。	签收环节	登记环节	初审环节	核发环节
2553	单项选择题	在GM/T 0071《电子文件密码应用指南》中，文件内容解密操作方法中，可以从（ ）中获取加密电子文件的对称算法和非对称算法标识。	安全属性	印章属性	元数据属性	标识属性
2554	单项选择题	在GM/T 0071《电子文件密码应用指南》中，文件内容的真实性不由（ ）的数字签名来保证。	签批属性	文件属性	水印属性	印章属性
2555	单项选择题	在GM/T 0071《电子文件密码应用指南》中，在添加签名的过程中，使用业务操作者或应用系统的签名私钥对（ ）进行数字签名。	文件内容明文	杂凑算法标识	签名证书信息	文件内容明文的杂凑值
2556	单项选择题	在GM/T 0071《电子文件密码应用指南》中，在电子文件管理系统接收电子文件相关操作方法中，需要使用业务系统签名公钥验证文件包的（ ）。	签名值	摘要值	签名证书	密钥对

2557	单项选择题	在GM/T 0071《电子文件密码应用指南》中，根据电子文件交换双方的身份不同，下列（ ）不属于正确的交换分类。	业务系统内部交换	业务系统间交换	业务系统与电子文件长期保存系统间交换	业务系统与电子文件管理系统间交换
2558	单项选择题	在GM/T 0071《电子文件密码应用指南》中，业务系统与电子文件管理系统交换时，将多个文件按预定规则进行组装形成文件包，对文件包整体做机密性、完整性、真实性保护，而对单个电子文件仅保留（ ）保护。	机密性和完整性	完整性和真实性	机密性和真实性	机密性
2559	多项选择题	GM/T 0071《电子文件密码应用指南》指出电子文件的文件内容解密操作方法，下面选项正确的有（ ）。	从安全属性中获取加密电子文件的对称算法和非对称算法标识	根据对称算法标识调用对称解密服务，使用加密公钥解密加密后的对称密钥，得到对称密钥	根据非对称算法标识调用非对称解密服务，使用加密私钥解密加密后的对称密钥，得到对称密钥	根据对称算法标识调用对称解密服务，对加密后的文件内容进行解密
2560	多项选择题	在GM/T 0071《电子文件密码应用指南》中，电子文件的文件内容完整性保护，进行签名操作步骤包括（ ）。	获取签名算法、杂凑算法标识	调用杂凑算法服务对文件内容明文计算摘要	使用业务操作者或应用系统的签名私钥对摘要值进行签名	将签名值、算法标识和签名证书按顺序填充至安全属性中
2561	多项选择题	GM/T 0071《电子文件密码应用指南》中指出，电子文件的安全性由（ ）共同保证。	文件内容的安全性	文件属性的安全性	文件大小	文件类型
2562	多项选择题	GM/T 0071《电子文件密码应用指南》指出电子文件的文件内容加密操作方法，下面选项正确的有（ ）。	获取对称算法、非对称算法标识；调用通用密码服务产生对称密钥	调用对称加密服务使用对称密钥加密文件内容；调用非对称加密服务使用电子文件接收者或应用系统加密公钥加密对称密钥	将加密后的对称密钥、对称密钥加密后的文件内容按数字信封格式封装，形成加密文件内容	将算法标识、算法模式、反馈位数存储在安全属性中

2563	判断题	在GM/T 0071《电子文件密码应用指南》中，电子文件中的标识属性是文件的唯一标识。	正确	错误		
2564	判断题	根据GM/T 0071《电子文件密码应用指南》，在电子文件密码应用中，应用系统采用身份鉴别机制，实现用户、系统的单向或双向身份鉴别服务，保证用户、系统身份的真实性。	正确	错误		
2565	判断题	根据GM/T 0071《电子文件密码应用指南》，在电子文件密码应用中，文件属性由应用系统自行维护时，可采用对文件内容进行签名的方式保证文件内容的机密性。	正确	错误		
2566	判断题	根据GM/T 0071《电子文件密码应用指南》，在电子文件密码应用中，文件属性采用标签方式组织时，采用对标签进行签名操作的方式，保证文件属性的完整性。	正确	错误		
2567	判断题	根据GM/T 0071《电子文件密码应用指南》，在电子文件密码应用中，文件属性由系统自行维护时，系统应用可采用密封数字信封方式，对元数据属性等需要保护的属性信息进行加解密操作。	正确	错误		
2568	判断题	根据GM/T 0071《电子文件密码应用指南》，在电子文件密码应用中，在添加签名过程中，根据签名算法标识调用签名验证服务，使用签名私钥和摘要值验证文件内容的签名值。	正确	错误		
2569	多项选择题	在GM/T 0071《电子文件密码应用指南》中，电子文件的文件内容完整性保护时，验证签名值过程正确的是（ ）。	从安全属性中获取杂凑算法、签名算法标识、签名证书信息和签名值	调用杂凑算法服务对文件内容计算摘要，将所有摘要按照既定规则进行组装	调用杂凑算法服务对组装后的数据计算HMAC	调用签名验证服务，使用签名公钥和摘要验证文件内容的签名值

2570	判断题	根据GM/T 0071《电子文件密码应用指南》，在电子文件密码应用中，文件属性（不含日志属性）形成或更新时，在签名操作过程中，调用杂凑算法服务对除印章属性外的其他属性计算摘要。	正确	错误		
2571	单项选择题	在GM/T 0011《可信计算 可信密码支撑平台功能与接口规范》中，采用的椭圆曲线密码算法为（）。	ECC256	ECC384	SM2	ECDAA
2572	单项选择题	在GM/T 0011《可信计算 可信密码支撑平台功能与接口规范》中，SM4算法采用的工作模式为（）。	ECB	CBC	CFB	OFB
2573	单项选择题	在GM/T 0011《可信计算 可信密码支撑平台功能与接口规范》中，计算度量值的过程应是执行（）的过程。	加密	解密	杂凑	签名
2574	单项选择题	在GM/T 0011《可信计算 可信密码支撑平台功能与接口规范》中，完整性报告是指平台向验证者提供平台或部分部件的完整性( )的过程 。	加密数据	解密数据	度量值	签名值
2575	单项选择题	在GM/T 0011《可信计算 可信密码支撑平台功能与接口规范》中,可信计算密码支撑平台采用EK标识其身份，在平台所有者授权下，在TCM内部生成一个( )密钥对，作为PIK，用于对TCM内部的信息进行数字签名。	AES	SM9	SM2	SM4
2576	单项选择题	在GM/T 0011《可信计算 可信密码支撑平台功能与接口规范》中,将数据与特定的( )及可信密码模块绑定在一起，这种操作称为数据封装。	平台状态(PCR值)	对称密钥	EK公钥	EK私钥

2577	单项选择题	在GM/T 0011《可信计算 可信密码支撑平台功能与接口规范》中，为防止TCM成为计算平台的性能瓶颈，将子系统中需执行保护的函数与无需执行保护的函数划分开，将无需执行保护的功能函数由计算平台主处理器执行，而这些支持函数构成了( )。	TCM	TDDL	TCM服务模块	可信计算
2578	单项选择题	在GM/T 0011《可信计算 可信密码支撑平台功能与接口规范》中,平台身份密钥代表平台身份，用于对可信计算密码支撑平台内部产生的数据进行( )。	加密	解密	杂凑	签名
2579	单项选择题	在GM/T 0011《可信计算 可信密码支撑平台功能与接口规范》中,在激活PIK证书的过程中，可信密码模块使用（ ），解密得到平台身份密钥的公钥的杂凑值和随机生成的对称加密密钥。	密码模块密钥的私钥	对称密钥	共享密钥	密码模块密钥的公钥
2580	单项选择题	在GM/T 0011《可信计算 可信密码支撑平台功能与接口规范》中，可信计算密码支撑平台以（ ）为可信根。	可信密码模块	可信存储	可信度量	可信报告
2581	多项选择题	在GM/T 0011《可信计算 可信密码支撑平台功能与接口规范》中，TSM设计的目标包括（ ）。	为应用程序调用TCM安全保护功能提供一个入口点	提供对TCM的同步访问	向应用程序隐藏TCM所建立的功能命令	管理TCM资源
2582	多项选择题	在GM/T 0011《可信计算 可信密码支撑平台功能与接口规范》中，以下（ ）是SM2引擎的功能。	产生SM2密钥对	执行SM2加/解密	执行SM2签名运算	杂凑运算
2583	多项选择题	在GM/T 0011《可信计算 可信密码支撑平台功能与接口规范》中，可信计算平台由（ ）组成。	TCM(可信密码模块)	TSM(TCM服务模块)	TCS(TCM核心服务)	TSP(TCM应用服务)

2584	多项选择题	在GM/T 0011《可信计算 可信密码支撑平台功能与接口规范》中，外部实体可以向平台请求验证平台的完整性。验证者验证平台完整性包括（ ）。	验证者得到平台发送的PCR值，PIK对PCR值的签名和PIK证书	验证者验证PIK证书	验证者验证PCR值的签名	验证者对PCR的值与平台的完整性基准值进行比较，若相同，则表明当前平台处于可信状态
2585	单项选择题	在GM/T 0011《可信计算 可信密码支撑平台功能与接口规范》中，可信计算密码支撑平台以可信密码模块为可信根,不能通过( )机制及平台自身安全管理功能,实现平台安全功能。	以可信度量根为起点，计算系统平台完整性度量值，建立计算机系统平台信任链，确保系统平台可信	可信报告根标识平台身份的可信，具有唯一性，以可信报告根为基础，实现平台身份证明和完整性报告	基于可信存储根，实现密钥管理、平台数据安全保护功能，提供相应的密码服务	利用外部密码机，通过对系统平台组件的完整性度量，确保系统平台完整性，并向外部实体可信地报告平台完整性
2586	多项选择题	在GM/T 0011《可信计算 可信密码支撑平台功能与接口规范》中，外部实体可以向平台请求验证平台的完整性。平台报告其完整性包括（ ）。	平台启动后，外部实体向平台发送完整性度量报告的请求	可信密码模块收集PCR的值，使用平台身份密钥（PIK）对PCR的值进行签名	平台将PCR的值，PIK对PCR值的签名和PIK证书发送给验证者	可信密码模块将PCR的值进行加密
2587	多项选择题	在GM/T 0011《可信计算 可信密码支撑平台功能与接口规范》中，可信计算密码支撑平台利用密码机制，通过对系统平台组件的( )，确保平台完整性。	完整性度量	完整性存储与报告	加解密	签名验签
2588	多项选择题	在GM/T 0011《可信计算 可信密码支撑平台功能与接口规范》中,涉及的密码机制包括（ ）。	SM2非对称密码算法和SM4对称密码算法	SM3密码杂凑算法	HMAC消息认证码算法	随机数生成
2589	判断题	在GM/T 0011《可信计算 可信密码支撑平台功能与接口规范》中，用于数据安全保护的密钥分为对称密钥和非对称密钥。	正确	错误		

2590	判断题	在GM/T 0011《可信计算 可信密码支撑平台功能与接口规范》中，密钥管理包括：密钥生成、密钥加载、密钥销毁、密钥导入、密钥迁移、密钥协商等功能。	正确	错误		
2591	判断题	在GM/T 0011《可信计算 可信密码支撑平台功能与接口规范》中，数据安全保护方式包括：数据加解密、数据封装、数字信封等方式。	正确	错误		
2592	判断题	在GM/T 0011《可信计算 可信密码支撑平台功能与接口规范》中，密码模块密钥可以由厂商（代理商）或者用户生成。	正确	错误		
2593	判断题	在GM/T 0011《可信计算 可信密码支撑平台功能与接口规范》中，存储主密钥必须在获取平台所有权时生成，为SM4对称密钥，平台所有者生成存储主密钥时，必须在可信密码模块内部生成。	正确	错误		
2594	判断题	在GM/T 0011《可信计算 可信密码支撑平台功能与接口规范》中，数据加解密只能采用对称密码算法，不能采用非对称加密算法实现。	正确	错误		
2595	判断题	在GM/T 0011《可信计算 可信密码支撑平台功能与接口规范》中，一个可信计算密码支撑平台只能产生1个PIK，PIK均与EK绑定，对外代表平台身份。	正确	错误		
2596	判断题	在GM/T 0011《可信计算 可信密码支撑平台功能与接口规范》中，规定了随机数生成的具体算法。	正确	错误		
2597	判断题	GM/T 0011《可信计算可信密码支撑平台功能与接口规范》中，可信密码模块是可信计算平台的硬件模块，为可信计算平台提供密码运算功能，具有受保护的存储空间。	正确	错误		

2598	判断题	GM/T 0011《可信计算可信密码支撑平台功能与接口规范》中，可信计算密码支撑平台内部的软件模块，为对平台外部提供访问可信密码模块的软件接口。	正确	错误		
2599	单项选择题	在GM/T 0058《可信计算 TCM服务模块接口规范》中，（ ）不属于TCM服务模块软件架构。	TCM应用服务	TCM核心服务	TCM设备驱动库	TSB软件基
2600	单项选择题	在GM/T 0058《可信计算 TCM服务模块接口规范》中，TCM核心服务是以（ ）形式存在，为TSP等上层应用提供TCM使用和密钥管理等功能接口。	系统服务	系统进程	系统驱动	可执行程序
2601	单项选择题	在GM/T 0058《可信计算 TCM服务模块接口规范》中，TCM设备驱动库位于（ ）和TCM设备驱动层之间。	TCM应用服务	TCM核心服务	可执行程序	TSB软件基
2602	单项选择题	在GM/T 0058《可信计算 TCM服务模块接口规范》中，（ ）为应用程序提供接口。	TCM应用服务	TCM核心服务	TCM设备驱动库	TSB软件基
2603	单项选择题	在GM/T 0058《可信计算 TCM服务模块接口规范》中，TCM应用服务属于（ ）。	用户进程	系统进程	内核软件	硬件
2604	单项选择题	在GM/T 0058《可信计算 TCM服务模块接口规范》中，TCM核心服务服务属于（ ）。	用户进程	系统进程	内核软件	硬件
2605	单项选择题	在GM/T 0058《可信计算 TCM服务模块接口规范》中，TCM设备驱动库属于（ ）。	用户进程	系统进程	内核软件	硬件
2606	单项选择题	在GM/T 0058《可信计算 TCM服务模块接口规范》中，以下（ ）不是该规范中支持的算法。	SM2	SM3	SM4	SM9
2607	单项选择题	在GM/T 0058《可信计算 TCM服务模块接口规范》中，（ ）获得由TCM产生的随机数。	Tspi_GetCapability	Tspi_GetRandom	Tspi_GetEvent	Tspi_GetTestResult

2608	多项选择题	在GM/T 0058《可信计算 TCM服务模块接口规范》中，TCM服务模块由（ ）组成。	TCM应用服务	TCM核心服务	TCM设备驱动库	TSB软件基
2609	多项选择题	在GM/T 0058《可信计算 TCM服务模块接口规范》中，NV存储管理类接口可用于NV区域的（ ）。	定义	读	写	释放
2610	多项选择题	在GM/T 0058《可信计算 TCM服务模块接口规范》中，类与对象的关系中，授权对象包括（ ）。	TCM对象	密钥对象	NV存储对象	迁移数据对象
2611	多项选择题	在GM/T 0058《可信计算 TCM服务模块接口规范》中，以下（ ）是该规范中支持的算法。	SM2	SM3	SM4	SM9
2612	多项选择题	在GM/T 0058《可信计算 TCM服务模块接口规范》中，类与对象的关系中，工作对象可以分为（ ）。	授权工作对象	非授权工作对象	NV存储对象	迁移数据对象
2613	判断题	在GM/T 0058《可信计算 TCM服务模块接口规范》中，TCM应用服务属于TCM服务模块软件架构，向应用程序提供TCM的服务。	正确	错误		
2614	判断题	在GM/T 0058《可信计算 TCM服务模块接口规范》中，TCM核心服务按照功能可以分为11个模块。	正确	错误		
2615	判断题	在GM/T 0058《可信计算 TCM服务模块接口规范》中，提供授权操作和非授权操作的接口。	正确	错误		
2616	判断题	在GM/T 0058《可信计算 TCM服务模块接口规范》中，NV存储管理类接口只能对NV区域进行定义及读写操作，不能进行NV区域的释放操作。	正确	错误		
2617	判断题	在GM/T 0058《可信计算 TCM服务模块接口规范》中，工作对象分为授权工作对象和非授权工作对象。	正确	错误		
2618	判断题	在GM/T 0058《可信计算 TCM服务模块接口规范》中，TDDL设备驱动库提供了获得TCM硬件、固件或者设备驱动的特征参数的接口。	正确	错误		

2619	判断题	在GM/T 0058《可信计算 TCM服务模块接口规范》中，策略管理类只能为一个用户应用程序配置相应的安全策略与行为。	正确	错误		
2620	判断题	在GM/T 0058《可信计算 TCM服务模块接口规范》中，每个上下文只能有一个TCM管理类的实例。	正确	错误		
2621	多项选择题	在GM/T 0058《可信计算 TCM服务模块接口规范》中，可信计算体系包含以下哪些标准（ ）。	可信计算密码支撑平台功能与接口规范	可信计算 TCM服务模块规范	可信计算 可信密码模块接口规范	可信计算 可信密码模块符合性检测规范
2622	单项选择题	在GM/T 0058《可信计算 TCM服务模块接口规范》中，TDDL是存在于（ ）之间的模块。	TDD(TCM设备驱动程序)和TSP(TCM应用服务)	TCS(TCM核心服务)和TDD(TCM设备驱动程序)	TSPTSP(TCM应用服务) 和TCS(TCM核心服务)	TSM(TCM服务模块)和TDD(TCM设备驱动程序)
2623	判断题	在GM/T 0058《可信计算 TCM服务模块接口规范》中，本标准适用于基于TCM的应用开发、使用及检测提供依据和指导。	正确	错误		
2624	判断题	在GM/T 0058《可信计算 TCM服务模块接口规范》中，TCS位于TSM服务提供者(TSP)层和TCM设备驱动库（TDDL）层之间，以系统服务的形式存在，为TSP等上层应用提供TCM使用和密钥管理等功能接口。	正确	错误		
2625	单项选择题	根据GM/T 0034《基于SM2密码算法的证书认证系统密码及其相关安全技术规范》，密钥管理中心中，密钥的保存期应大于（ ）。	3年	5年	8年	10年
2626	单项选择题	根据GM/T 0034《基于SM2密码算法的证书认证系统密码及其相关安全技术规范》，根CA的数字证书由（ ）签发。	上级CA	下级CA	地方CA	根CA自己
2627	单项选择题	根据GM/T 0034《基于SM2密码算法的证书认证系统密码及其相关安全技术规范》，非根CA的数字证书由（ ）签发。	根CA	上级CA	地方CA	下级CA自己

2628	单项选择题	在GM/T 0034《基于SM2密码算法的证书认证系统密码及其相关安全技术规范》中，以下哪项不是密钥管理系统的备份措施（ ）。	热备份	异地备份	冷备份	密钥分发
2629	单项选择题	在GM/T 0034《基于SM2密码算法的证书认证系统密码及其相关安全技术规范》中，以下哪种类型不是密钥库管理模块按照储存的密钥状态去划分的类型（ ）。	备用库	在用库	证书库	历史库
2630	单项选择题	在GM/T 0034《基于SM2密码算法的证书认证系统密码及其相关安全技术规范》中，KMC与CA之间采用怎样的身份鉴别机制（ ）。	账户名密码鉴别机制	双向身份鉴别机制	生物学鉴别机制	单向身份鉴别机制
2631	单项选择题	在GM/T 0034《基于SM2密码算法的证书认证系统密码及其相关安全技术规范》中，CA提供的服务中，RA的建设方式可以是哪一种（ ）。	部分托管在CA，部分在远端	全部建设在远端	全部托管在签名验签服务器内	全部托管在安全认证网关内
2632	单项选择题	在GM/T 0034《基于SM2密码算法的证书认证系统密码及其相关安全技术规范》中，以下哪种协议不是CA系统对用户接口要求的协议标准（ ）。	HTTP	LDAP	OAuth2.0	OCSP
2633	多项选择题	在GM/T 0034《基于SM2密码算法的证书认证系统密码及其相关安全技术规范》中，安全管理系统的日志记录主要包括（ ）。	操作项目	操作起始时间	操作终止时间	操作结果
2634	多项选择题	在GM/T 0034《基于SM2密码算法的证书认证系统密码及其相关安全技术规范》中，证书状态查询有几种提供服务的方式（ ）。	OCSP查询	CRL查询	EMAIL查询	官网查询
2635	多项选择题	在GM/T 0034《基于SM2密码算法的证书认证系统密码及其相关安全技术规范》中，按证书的功能分类，证书分为哪几类（ ）。	设备证书	人员证书	加密证书	签名证书

2636	多项选择题	根据GM/T 0034《基于SM2密码算法的证书认证系统密码及其相关安全技术规范》，证书认证系统的总体设计原则如下（ ）。	证书认证系统遵循标准化、模块化设计原则	证书认证系统设置相对独立的功能模块，通过各模块之间的安全连接，实现各项功能	各模块之间的通信采用基于身份鉴别机制的安全通信协议	各模块使用的密码运算都必须在密码设备中完成
2637	多项选择题	根据GM/T 0034《基于SM2密码算法的证书认证系统密码及其相关安全技术规范》，证书认证系统对数字证书的哪些步骤全生命周期进行管理的系统（ ）。	签发	发布	更新	撤销
2638	多项选择题	在GM/T 0034《基于SM2密码算法的证书认证系统密码及其相关安全技术规范》中，CA系统的计算机网络需要合理分段，原则上要求整个网络划分为（ ）。	公共部分	服务部分	管理部分	核心部分
2639	判断题	根据GM/T 0034《基于SM2密码算法的证书认证系统密码及其相关安全技术规范》，SM2算法中，数字签名证书和数据加密证书使用的密钥是同一对。	正确	错误		
2640	判断题	根据GM/T 0034《基于SM2密码算法的证书认证系统密码及其相关安全技术规范》，证书申请可采用在线或离线两种方式。	正确	错误		
2641	判断题	根据GM/T 0034《基于SM2密码算法的证书认证系统密码及其相关安全技术规范》，证书签发系统负责证书/证书撤销列表的生成。	正确	错误		
2642	判断题	根据GM/T 0034《基于SM2密码算法的证书认证系统密码及其相关安全技术规范》，在证书的使用过程中，应用系统只能通过检查CRL/ARL，获取有关证书的状态。	正确	错误		

2643	判断题	根据GM/T 0034《基于SM2密码算法的证书认证系统密码及其相关安全技术规范》，数字证书中，证书颁发者用私钥对证书内容进行签名，再将证书和签名一起发布。	正确	错误		
2644	判断题	根据GM/T 0034《基于SM2密码算法的证书认证系统密码及其相关安全技术规范》，安全管理系统主要包括监控运维系统和安全防护系统。	正确	错误		
2645	判断题	根据GM/T 0034《基于SM2密码算法的证书认证系统密码及其相关安全技术规范》，安全审计与评估规范，规定了CA运行系统的审核范围和评价标准。	正确	错误		
2646	判断题	根据GM/T 0034《基于SM2密码算法的证书认证系统密码及其相关安全技术规范》，根据CA的请求为用户生成对称密钥,该密钥由密钥管理系统的硬件密码设备生成。	正确	错误		
2647	判断题	根据GM/T 0034《基于SM2密码算法的证书认证系统密码及其相关安全技术规范》，证书验证是指按照验证策略确认证书有效性和真实性的过程。	正确	错误		
2648	单项选择题	在GM/T 0034《基于SM2密码算法的证书认证系统密码及其相关安全技术规范》中，关于CA管理和操作人员的叙述不正确的是（ ）。	超级管理员负责CA系统的策略设置	业务管理员负责CA系统的某个子系统的业务管理	审计管理员负责对涉及系统安全的事件和各类管理和操作人员的行为进行审计和监督	业务操作员按其权限进行具体的业务操作
2649	单项选择题	在GM/T 0034《基于SM2密码算法的证书认证系统密码及其相关安全技术规范》中，CA和KMC的根密钥需要用密钥分割或秘密共享机制分割，（ ）不能成为分管者。	业务操作员	业务管理员	系统维护人员	以上都是

2650	单项选择题	在GM/T 0034《基于SM2密码算法的证书认证系统密码及其相关安全技术规范》中，关于密钥库以下说法不正确的是（ ）。	密钥库中的密钥数据应加密存放	分为备用库、在用库和历史库	CA申请的密钥从在用库中取出	历史库存放过期或已被注销的密钥对
2651	单项选择题	在GM/T 0034《基于SM2密码算法的证书认证系统密码及其相关安全技术规范》中，关于安全操作与维护，以下说法不正确的是（ ）。	改变系统的配置如无上级主管批准，操作时应有双人在场	系统出现故障时，应由系统管理人员检查处理，其它人员未经批准不得处理	对CA系统的每次操作都应记录	未经批准不得在服务器上安装任何软件
2652	多项选择题	在GM/T 0034《基于SM2密码算法的证书认证系统密码及其相关安全技术规范》中，密钥管理系统的密钥生成模块应具有（ ）功能。	非对称密钥对的生成	对称密钥的生成	随机数的生成	备用库密钥不足时自动补充
2653	多项选择题	在GM/T 0034《基于SM2密码算法的证书认证系统密码及其相关安全技术规范》中，证书的管理安全应满足（ ）要求。	证书申请者的身份应通过验证	由RA签发与申请者身份相符的证书	可以通过审计日志对证书事件进行跟踪	对于证书的任何处理都应作日志记录
2654	单项选择题	在GM/T 0034《基于SM2密码算法的证书认证系统密码及其相关安全技术规范》中，关于证书认证中心的管理区的说法不正确的是（ ）。	进入管理区的人员只需使用身份识别卡	所有的墙体应采用高强度防护墙	管理区所有的房间不应安装窗户	人员进出管理区要有日志记录
2655	判断题	根据GM/T 0034《基于SM2密码算法的证书认证系统密码及其相关安全技术规范》，RA的业务管理员应由CA业务管理员管理。	正确	错误		
2656	判断题	在GM/T 0034《基于SM2密码算法的证书认证系统密码及其相关安全技术规范》中，所有密钥恢复操作都应由密钥管理中心业务操作员和司法取证人员同时在场。	正确	错误		
2657	判断题	在GM/T 0034《基于SM2密码算法的证书认证系统密码及其相关安全技术规范》中，证书认证中心对数据变化量少的服务器，可每周做一次备份。	正确	错误		

2658	单项选择题	根据GM/T 0014《数字证书认证系统密码协议规范》，LDAP允许证书订户的（ ）行为。	插入	查询	修改	删除
2659	单项选择题	根据GM/T 0014《数字证书认证系统密码协议规范》，在数字证书认证系统协议流程中，下列关于RA的说法不正确的是（ ）。	受理用户证书申请	对用户证书申请进行形式审查	证书数据验证	签发证书
2660	单项选择题	在数字证书认证系统中，KM指的是（ ）。	密钥生成中心	密钥备份系统	密钥托管系统	密钥管理系统
2661	单项选择题	根据GM/T 0014《数字证书认证系统密码协议规范》，下列选项不属于KM接收CA系统的密钥服务请求的是（ ）。	申请密钥对	恢复密钥对	删除密钥对	撤销密钥对
2662	单项选择题	根据GM/T 0014《数字证书认证系统密码协议规范》，如果OCSP接收到一个没有遵循OCSP语法的请求，应做如下响应（ ）。	忽略该请求	回复“未正确格式化的请求”	回复“内部错误”	回复“稍后再试”
2663	单项选择题	在数字证书认证系统中，终端用户签名私钥在（ ）生成。	终端用户证书载体	密钥管理系统	CA	RA
2664	单项选择题	在数字证书认证系统中，终端用户加密私钥在（ ）生成。	终端用户证书载体	密钥管理系统	CA	RA
2665	单项选择题	根据GM/T 0014《数字证书认证系统密码协议规范》，向OCSP查询一张被冻结的证书，OCSP返回的证书状态为（ ）。	未知	已冻结	已撤销	良好
2666	单项选择题	根据GM/T 0014《数字证书认证系统密码协议规范》，向OCSP查询一张被挂起的证书，OCSP返回的证书状态为（ ）。	未知	已挂起	已撤销	良好
2667	单项选择题	根据GM/T 0014《数字证书认证系统密码协议规范》，OCSP查询返回的证书状态不包括下列选项中的（ ）。	已冻结	已撤销	未知	良好

2668	多项选择题	根据GM/T 0014《数字证书认证系统密码协议规范》，KM接收CA系统的密钥服务请求包括下列选项中的（ ）。	申请密钥对	恢复密钥对	查询密钥对	撤销密钥对
2669	多项选择题	LDAP在PKI中主要用来存放下列选项中的（ ）。	证书	签名	证书撤销列表	公钥
2670	多项选择题	根据GM/T 0014《数字证书认证系统密码协议规范》，在数字证书认证系统协议流程中，下列关于KM的说法正确的是（ ）。	接收CA的申请密钥对请求	接收CA的恢复密钥对请求	接收CA的撤销密钥对请求	向LDAP发布证书和证书撤销链
2671	多项选择题	根据GM/T 0014《数字证书认证系统密码协议规范》，CA向KM发送的密钥服务请求数据包括下列选项中的（ ）。	协议版本	CA标识符	扩展的请求信息	请求信息的签名
2672	多项选择题	根据GM/T 0014《数字证书认证系统密码协议规范》，KM对来自CA请求的处理响应包括下列选项中的（ ）。	协议版本	KM标识符	响应信息	响应信息的签名
2673	多项选择题	根据GM/T 0014《数字证书认证系统密码协议规范》，一个OCSP请求包含下列选项中的（ ）。	协议版本	服务请求	目标证书标识	可选扩展
2674	多项选择题	根据GM/T 0014《数字证书认证系统密码协议规范》，用户申请证书需要向RA/CA提供下列选项中的（ ）。	用户信息	用户签名公钥	用户加密公钥	用户加密私钥
2675	多项选择题	根据GM/T 0014《数字证书认证系统密码协议规范》，OCSP查询返回的证书状态包括（ ）。	已冻结	已撤销	未知	良好
2676	多项选择题	根据GM/T 0014《数字证书认证系统密码协议规范》，在数字证书认证系统协议流程中，下列关于CA的说法正确的是（ ）。	向KM申请加密密钥对	签发签名证书	签发加密证书	生成加密密钥对
2677	单项选择题	根据GM/T 0014《数字证书认证系统密码协议规范》，在数字证书认证系统协议流程中，下列关于CA的说法错误的是（ ）。	向KM申请加密密钥对	签发签名证书	签发加密证书	生成加密密钥对

2678	判断题	GM/T 0014《数字证书认证系统密码协议规范》适用于对于组织或机构内部使用的数字证书认证系统密码协议的建设、运行及管理。	正确	错误		
2679	判断题	根据GM/T 0014《数字证书认证系统密码协议规范》，证书与证书撤销链发布是指CA把新签发的证书与证书撤销链送到LDAP目录服务器，以供用户查询、下载和上传。	正确	错误		
2680	判断题	根据GM/T 0014《数字证书认证系统密码协议规范》，OCSP使得应用程序可获得所需要检验证书的状态。	正确	错误		
2681	判断题	根据GM/T 0014《数字证书认证系统密码协议规范》，根CA证书中的主题域（subject）和签发者域（issuer）在特殊环境下可以不同。	正确	错误		
2682	判断题	根据GM/T 0014《数字证书认证系统密码协议规范》，不同的CA向KM申请密钥对时，可以提交相同的用户加密证书序列号。	正确	错误		
2683	单项选择题	GM/T 0014《数字证书认证系统密码协议规范》规范的方面不包括（ ）。	协议流程	密钥结构	数据格式	报文语法
2684	多项选择题	GM/T 0014《数字证书认证系统密码协议规范》的内容包括（ ）。	用户同CA之间的安全协议	CA同KM之间的安全协议	用户同LDAP之间的安全协议	CA与RA之间的安全协议
2685	判断题	在GM/T 0014《数字证书认证系统密码协议规范》中，封装结构应遵循GM/T 0009《SM2密码算法使用规范》。	正确	错误		
2686	单项选择题	GM/T 0037《证书认证系统检测规范》检测的证书认证服务运营系统应按照（ ）标准的要求进行建设。	GM/T 0034《基于SM2密码算法的证书认证系统密码及其相关安全技术规范》	GM/T 0014《数字证书认证系统密码协议规范》	GM/T 0015《基于SM2密码算法的数字证书格式规范》	GM/T 0031《安全电子签章密码技术规范》

2687	单项选择题	在GM/T 0037《证书认证系统检测规范》中，证书认证系统的（ ）应为屏蔽机房。	公共区	服务区	管理区	核心区
2688	单项选择题	在GM/T 0037《证书认证系统检测规范》中，对于证书认证系统的审计功能的检测，下列选项不正确的是（ ）。	应能够对事件发生的时间、事件操作者、操作类型、操作结果等信息进行审计	审计应能验证记录的签名	审计数据只能被审计员修改	审计过的记录应有明显标记
2689	单项选择题	在GM/T 0037《证书认证系统检测规范》中，对于产品检测，该项检测结果不符合要求即判定为不符合的是（ ）。	物理区域	系统初始化	CRL签发	系统性能
2690	单项选择题	在GM/T 0037《证书认证系统检测规范》中，对于项目检测，该项检测结果不符合要求即判定为不符合的是（ ）。	物理区域	系统初始化	CRL签发	系统性能
2691	单项选择题	在GM/T 0037《证书认证系统检测规范》中，证书认证系统采用的协议应符合（ ）标准的要求。	GM/T 0003.3《SM2椭圆曲线公钥密码算法 第3部分：密钥交换协议》	GM/T 0014《数字证书认证系统密码协议规范》	GB/T 38636《信息安全技术 传输层密码协议》	GM/T 0089《简单证书注册协议规范》
2692	单项选择题	在GM/T 0037《证书认证系统检测规范》中，证书认证服务运营系统中，对于设备的摆放以下错误的是（ ）。	注册审计终端放在管理区	注册管理服务器及连接的密码机放在服务区	LDAP查询服务器放在服务区	入侵检测控制台放在核心区
2693	单项选择题	在GM/T 0037《证书认证系统检测规范》中，证书认证系统采用的证书格式应符合（ ）的要求。	GM/T 0043《数字证书互操作检测规范》	GM/T 0014《数字证书认证系统密码协议规范》	GM/T 0015《基于SM2密码算法的数字证书格式规范》	GM/T 0092《基于SM2算法的证书申请语法规范》
2694	单项选择题	在GM/T 0037《证书认证系统检测规范》中，以下各项仅用于产品检测的是（ ）。	系统初始化	岗位及权限管理	多层结构支持	网络结构

2695	单项选择题	GM/T 0037《证书认证系统检测规范》中，对RA的定义是（ ）。	对数字证书的签发、发布、更新、撤销等数字证书全生命周期进行管理的系统	对数字证书注册流程进行全过程管理的系统	实现密钥管理功能的系统	以上皆不是
2696	单项选择题	GM/T 0037《证书认证系统检测规范》中RA对申请信息的审核，以下各项不正确的是（ ）。	应能提供对申请信息审核的界面	应能自动批量对申请信息进行审核	应能将审核不通过的信息返回到录入界面	应能自动使操作员对其操作行为进行签名
2697	单项选择题	GM/T 0037《证书认证系统检测规范》中，以下描述不正确的是（ ）。	RA应能提供证书下载	日志应能按操作者进行查询	审计数据仅能由审计员更改	证书认证系统应能通过密钥管理中心为已经注册的用户提供密钥恢复服务
2698	多项选择题	GM/T 0037《证书认证系统检测规范》中，证书认证系统的物理区域应划分为（ ）。	公共区	服务区	管理区	核心区
2699	多项选择题	GM/T 0037《证书认证系统检测规范》对网络配置安全策略的检测内容应包括（ ）。	防火墙	入侵检测	漏洞扫描	病毒防治
2700	多项选择题	证书签发系统应设置的岗位和权限包括（ ）。	业务管理员	业务操作员	审计管理员	审计员
2701	多项选择题	GM/T 0037《证书认证系统检测规范》中，证书注册系统对申请信息的录入需要检测的内容包括（ ）。	应能提供录入和修改证书申请信息的界面	应能选择所申请数字证书的密钥类型及长度	应支持批量证书申请信息的导入	应能自动使操作员对其操作行为进行签名
2702	多项选择题	GM/T 0037《证书认证系统检测规范》中，证书认证系统中日志应记录的内容包括（ ）。	事件发生的时间	事件的操作者	操作类型	操作结果
2703	多项选择题	GM/T 0037《证书认证系统检测规范》中对场地的检测方法包括（ ）。	尝试使用授权和未授权的门卡通过门禁	查看系统物理区域的划分	从监控屏查看机房的各个区域	查看屏蔽机房的验收报告
2704	多项选择题	GM/T 0037《证书认证系统检测规范》中，证书认证服务运营系统中，对于设备的摆放以下正确的是（ ）。	CRL的存储与发布服务器放在服务区	LDAP查询服务器放在管理区	CRL的生成与签发服务器放在核心区	在各区域间放置防火墙

2705	多项选择题	GM/T 0037《证书认证系统检测规范》中，证书认证服务运营系统中，对于设备的摆放以下错误的是（ ）。	在各区域间放置防火墙	注册管理服务器及连接的密码机放在服务区	入侵检测控制台放在核心区	LDAP查询服务器放在管理区
2706	多项选择题	GM/T 0037《证书认证系统检测规范》中，RA的功能包括下列选项中的（ ）。	应能进行申请信息的录入和修改	应能进行申请信息的审核	应能提供证书下载	应能对证书类型及内容进行定义
2707	多项选择题	GM/T 0037《证书认证系统检测规范》中，证书认证系统产品包括下列选项中的（ ）。	签发系统服务器	注册系统服务器	LDAP服务器	OCSP服务器
2708	判断题	GM/T 0037《证书认证系统检测规范》不仅适用于产品检测，也适用于项目检测。	正确	错误		
2709	判断题	GM/T 0037《证书认证系统检测规范》中，CA证书可以由CA给自己签发，也可以由另一个CA签发。	正确	错误		
2710	判断题	GM/T 0037《证书认证系统检测规范》中，证书认证系统可以采用B/S结构或C/S结构。	正确	错误		
2711	判断题	证书认证系统中密码机应通过独立的物理端口与服务器连接。	正确	错误		
2712	判断题	GM/T 0037《证书认证系统检测规范》中，当CA给RA授权的证书模板发生变化时，RA应能与CA进行模板同步更新。	正确	错误		
2713	判断题	GM/T 0037《证书认证系统检测规范》中，证书状态查询服务可以采用CRL查询或在线证书状态查询。	正确	错误		
2714	判断题	GM/T 0037《证书认证系统检测规范》中，对证书认证系统的产品检测，无需检测其是否能通过新CA证书与旧CA证书的证书链，实现新旧证书更替。	正确	错误		

2715	判断题	GM/T 0037《证书认证系统检测规范》中，对证书认证系统的产品检测，入根检测不合格即判定为不合格。	正确	错误		
2716	单项选择题	GM/T 0037《证书认证系统检测规范》，关于物理区域的检测以下说法不正确的是（）。	注册管理服务器及连接的密码机应放置在服务区	注册审计终端应放置在管理区	注册管理服务器及连接的密码机应放置在核心区	在各区域间应放置防火墙
2717	单项选择题	GM/T 0037《证书认证系统检测规范》，关于审计的检测以下说法正确的是（）。	应设置单独的审计管理终端	审计应能验证记录的签名	审计过的记录应有明显标记	以上都对
2718	多项选择题	GM/T 0037《证书认证系统检测规范》中，证书认证系统产品由（）组成。	RA服务器	密码机	KM服务器	OCSP服务器
2719	判断题	GM/T 0037《证书认证系统检测规范》中对网络结构进行检测时，采用B/S模式的网络应分为公共区、服务区/管理区、核心区三个网段。	正确	错误		
2720	单项选择题	GM/T 0051《密码设备管理 对称密钥管理技术规范》是密码设备管理系列规范之一，其建立密钥管理安全通道所依据的规范是（）。	GM/T 0050《密码设备管理 设备管理技术规范》	GM/T 0052《密码设备管理 VPN设备监察管理规范》	GM/T 0053《密码设备管理 远 监控与合规检验接口数据规范》	GM/T 0015《基于SM2算法 的数字证书格式规范》
2721	单项选择题	GM/T 0051《密码设备管理 对称密钥管理技术规范》中，被管密钥的范围是（）。	业务密钥	密码设备密钥	临时交互密钥	密钥管理密钥
2722	单项选择题	被管设备的对称密钥在GM/T 0051《密码设备管理 对称密钥管理技术规范》中，是以（）方式被传输。	原子密钥	自定义	文本格式	其它格式
2723	单项选择题	GM/T 0051《密码设备管理 对称密钥管理技术规范》中密钥管理应用的标识为（）。	0xC0	0xC1	0xC2	0xC3
2724	单项选择题	以下选项不属于GM/T 0051《密码设备管理 对称密钥管理技术规范》中密钥管理中心的功能的是（）。	主控模块	密钥生成及管理模块	密钥封装及分发模块	密钥管理代理模块

2725	单项选择题	关于原子密钥的描述，以下选项不正确的是（ ）。	原子密钥可以是通用密钥产生装置生成的随机密钥	原子密钥可以是专用密钥产生装饰生成的专用格式密钥	原子密钥可以是临时密钥	原子密钥需经过标准封装后进行分发
2726	单项选择题	GM/T 0051《密码设备管理 对称密钥管理技术规范》中，密钥管理主机不包括以下功能中的（ ）。	密钥管理应用	密码设备管理平台	密钥设备管理接口	对业务提供密码服务
2727	单项选择题	以下描述不符合密钥库功能的是（ ）。	密钥在密钥库中经过本地主密钥加密存储	密钥需随用随生成	由密钥生成策略触发生成	存储的密钥已完成标准化封装
2728	单项选择题	在GM/T 0051《密码设备管理 对称密钥管理技术规范》中，密钥管理系统初始化，不包含以下功能中的（ ）。	密码设备管理平台功能	用户激活功能	密钥管理中心证书注册	被管设备证书注册
2729	单项选择题	在GM/T 0051《密码设备管理 对称密钥管理技术规范》中，从密钥库中取出密钥并下发的流程，以下描述不正确的是（ ）。	待分发密钥被主密钥加密	由密码设备将待分发密钥转换为本次会话的分发保护密钥加密	密钥转加密可以在数据库中完成	对密钥进行标准封装后下发
2730	多项选择题	以下密码设备可被GM/T 0051《密码设备管理 对称密钥管理技术规范》管理的是（ ）。	密码机	密码卡	智能IC卡	智能密码钥匙
2731	多项选择题	在GM/T 0051《密码设备管理 对称密钥管理技术规范》中，密钥生成装置包含的种类有（ ）。	满足规范要求的通用密钥生成装置	满足规范要求的专用密钥生成装置	自定义密钥生成装置	以上都是
2732	多项选择题	GM/T 0051《密码设备管理 对称密钥管理技术规范》中的密钥管理系统制定的管理策略包含（ ）。	密钥生成策略，包括生成装置种类、密钥数量、密钥长度等	密钥分发策略，包括在线密钥分发、离线密钥分发等	密钥封装格式、导入处理方式	设备属性信息

2733	多项选择题	在GM/T 0051《密码设备管理 对称密钥管理技术规范》中，密钥生成模块的设计要求包括（ ）。	为多个系统提供业务密钥	密钥生成装置为硬件设备，随机数质量满足国家标准GB/T 32915《信息安全技术 二元序列随机性检测方法》	支持外部密钥的导入	支持密钥以密文方式导出，明文密钥不可出硬件设备
2734	多项选择题	在GM/T 0051《密码设备管理 对称密钥管理技术规范》中，被管密码设备的技术要求包括（ ）。	由设备管理代理接收密钥管理指令，由密钥管理代理处理密钥管理操作	与设备管理结合，根据密钥状态支持密钥申请主动上报	支持标准密钥管理协议，将标准密钥封装解析为密码设备可识别的原子密钥	对于存量密码设备，支持将标准密钥管理协议适配转换为存量设备专用密钥管理指令
2735	多项选择题	在GM/T 0051《密码设备管理 对称密钥管理技术规范》中，密钥管理指令PDU的类型包括（ ）。	分发保护密钥协商指令和密钥分发指令	密钥销毁指令	密钥启用指令	密钥申请指令
2736	多项选择题	在GM/T 0051《密码设备管理 对称密钥管理技术规范》中，完整的密钥产生和下发操作，需要的接口包含以下选项中的（ ）。	密钥生成装置接口	密钥管理应用的指令发送接口	被管设备密钥管理接口	密码设备自定义接口
2737	多项选择题	在GM/T 0051《密码设备管理 对称密钥管理技术规范》中，在线密钥管理的总体思路是（ ）。	由密钥生成装置产生被管设备所需原子密钥，由密管密码设备与密码生成装置协商会话密钥加密并传输至密钥管理中心	密钥分发调用密钥管理平台安全通道API，根据分发策略，以标准格式封装原子密钥发送至被管设备	被管设备的设备管理代理获取密钥管理指令，由密钥管理代理处理密钥管理指令	本标准不支持离线设备的密钥管理

2738	多项选择题	在GM/T 0051《密码设备管理 对称密钥管理技术规范》中，以下选项属于密钥管理审计内容的是（）。	对密钥生成、存储、分发等密钥管理事件，以及策略管理、身份认证等系统管理事件进行审计	对用户主动操作的管理事件进行审计	记录服务器状态	对服务器状态进行审计
2739	判断题	在GM/T 0051《密码设备管理 对称密钥管理技术规范》中，密钥恢复包括用户恢复与司法恢复两种。	正确	错误		
2740	判断题	在GM/T 0051《密码设备管理 对称密钥管理技术规范》中，密钥数据封装格式与分发方式无关。	正确	错误		
2741	判断题	在GM/T 0051《密码设备管理 对称密钥管理技术规范》中，密钥在任何时候不能以明文方式导出密码设备。	正确	错误		
2742	判断题	在GM/T 0051《密码设备管理 对称密钥管理技术规范》中，分发保护密钥是由密钥管理中心采用被管设备公钥加密保护下发。	正确	错误		
2743	判断题	在GM/T 0051《密码设备管理 对称密钥管理技术规范》中，密钥分发指令中只能一次分发一个密钥。	正确	错误		
2744	判断题	在GM/T 0051《密码设备管理 对称密钥管理技术规范》中，密钥生成装置接口中DataSign参数用于与密钥管理中心传输密钥的完整性保护。	正确	错误		
2745	判断题	在GM/T 0051《密码设备管理 对称密钥管理技术规范》中，被管设备的密钥管理接口用于具体型号设备的密钥处理，由密码设备厂商自定义。	正确	错误		
2746	单项选择题	GM/T 0051 《密码设备管理 对称密钥管理技术规范》主要功能是管理（ ）密钥。	密钥加密	主	设备	业务

2747	单项选择题	GM/T 0051《 密码设备管理 对称密钥管理技术规范》的密钥生成装置所生成密钥为（ ）密钥。	原子	密钥加密	主	业务
2748	单项选择题	GM/T 0051《 密码设备管理 对称密钥管理技术规范》中，下列选项中不属于密钥标准封装的内容的是（ ）。	管理节点标识	密钥长度	校验算法标识	封装时间
2749	多项选择题	GM/T 0051《 密码设备管理 对称密钥管理技术规范》中的原子密钥生成过程，可以由（ ）生成。	专用密钥生成装置	装置间协商产生	通用密钥生成装置	随机数发生器
2750	多项选择题	GM/T 0051《 密码设备管理 对称密钥管理技术规范》中，下列模块属于密钥管理系统的组成部分的是（ ）。	主控管理	密钥生成/封装/存储/分发管理	备份 / 恢复/归档管理	密管代理
2751	多项选择题	GM/T 0051《 密码设备管理 对称密钥管理技术规范》中，下列属于密钥管理系统的设计原则的是（ ）。	密钥管理系统遵循标准化、模块化、松耦合设计原则	应保障系统模块之间连接的安全性，包括完整性、机密性、防重放、不可否认性	系统可为多个被管系统提供业务密钥服务	各子系统之间的通信采用基于身份验证机制的安全通信协议
2752	判断题	GM/T 0051《 密码设备管理 对称密钥管理技术规范》中密钥加密转换只能在密码设备内进行，要求明文密钥不可导出密码设备	正确	错误		
2753	判断题	GM/T 0051《 密码设备管理 对称密钥管理技术规范》中的密钥库中的密钥必须加密存放或者采用分割明文存储方式。	正确	错误		
2754	单项选择题	GM/T 0008《安全芯片密码检测准则》中，安全等级1的安全芯片要求至少（ ）个相互独立的物理噪声源。	2个	4个	8个	1个
2755	单项选择题	GM/T 0008《安全芯片密码检测准则》中，下列哪项不属于安全等级1的安全芯片自检要求的是（ ）。	上电自检	复位自检	指令自检	主动自检

2756	单项选择题	GM/T 0008《安全芯片密码检测准则》中，下列选项属于安全等级1的安全芯片关于“审计”的要求的是（ ）。	安全芯片须具有相应的文档跟踪记录安全芯片所处的生命周期阶段	安全芯片须具有逻辑或物理的安全机制保证标识不被更改	安全芯片须具有唯一标识	安全芯片须定义芯片的生命周期，并对生命周期各阶段进行标识
2757	单项选择题	GM/T 0008《安全芯片密码检测准则》中，下列内容不属于安全等级2的安全芯片对公钥密码算法的要求的是（ ）。	在各种应用模式下实现正确	若公钥密码算法需要由安全芯片生成素数，则生成素数须通过素性检测	对于任何输入均能给出明确结果或响应	公钥密码算法的所有细节都采用专用硬件实现
2758	单项选择题	GM/T 0008《安全芯片密码检测准则》中，下列内容不属于安全等级2的安全芯片对固件存储的要求的是（ ）。	固件不得通过接口读出	除固件本身外，其他代码不得读写固件代码	安全芯片中的固件以密文形式存数	除固件本身外，其他代码读写固件中的数据需要相应的权限
2759	单项选择题	GM/T 0008《安全芯片密码检测准则》中，下列内容不属于安全等级1的安全芯片对密钥生成的要求的是（ ）。	能够正确有效的生成密钥	生成密钥不可预测不可逆推	密钥生成后立即清除密钥生成过程中使用过且不再需要使用的相关数据和临时信息	若安全芯片能够生成随机数，须使用安全芯片自身生成的随机数
2760	单项选择题	GM/T 0008《安全芯片密码检测准则》中，安全等级1的安全芯片要求安全芯片对密钥和（ ）提供基本的保护措施	固件	敏感信息	标识	随机数
2761	单项选择题	GM/T 0008《安全芯片密码检测准则》中，下列选项属于安全等级1的安全芯片故障攻击防护的要求的是（ ）。	无要求	防护措施有效性须通过检测	需通过文档或其他方式对响应的防护措施及其有效性进行描述和说明	安全芯片应能够发现电压、频率、温度等工作参数的改变
2762	单项选择题	GM/T 0008《安全芯片密码检测准则》中，关于安全芯片固件，以下说法错误的是（ ）。	安全芯片固件可以实现未声明的功能	安全芯片需要能够正确、有效地实现声明的功能	安全一级的安全芯片固件可以再次导入	安全芯片固件导入时应支持导入源的身份鉴别
2763	多项选择题	GM/T 0008《安全芯片密码检测准则》中，安全芯片接口分为（ ）。	逻辑接口	软件接口	物理接口	隐式接口

2764	多项选择题	GM/T 0008《安全芯片密码检测准则》中，安全芯片生成的密钥必须保证（ ）。	不可预测	使用非确定性数据	不可逆推	使用外部生成的随机数
2765	多项选择题	GM/T 0008《安全芯片密码检测准则》中，下列选项属于安全芯片敏感信息保护部分的要求的是（ ）。	敏感信息的存储	敏感信息的清除	敏感信息的运算	敏感信息的传输
2766	多项选择题	GM/T 0008《安全芯片密码检测准则》中，下列选项属于安全芯片固件安全部分的要求的是（ ）。	固件的存储	固件的执行	固件的导入	固件的备份
2767	多项选择题	GM/T 0008《安全芯片密码检测准则》中，下列内容属于安全等级2的安全芯片对审计的要求的是（ ）。	安全芯片必须具有唯一标识	唯一标识是可校验的	安全芯片具有逻辑或物理的安全机制保证标识不被更改	安全芯片可以具有重复的标识
2768	单项选择题	GM/T 0008《安全芯片密码检测准则》中，下列内容不属于安全芯片对生命周期的要求的是（ ）。	安全芯片可以没有生命周期模型	须定义安全芯片的生命周期，并对生命周期各阶段进行标识	须具有相应的文档跟踪记录安全芯片所处的生命周期阶段	须具有相应的管理机制维护安全芯片的生命周期，并根据生命周期阶段的变化进行相应的处理。
2769	多项选择题	GM/T 0008《安全芯片密码检测准则》中，下列内容属于安全等级2的安全芯片对能量分析攻击的要求的是（ ）。	安全芯片须具有相应措施保证算法运算时能量消耗特征与密钥和敏感信息之间没有明显的相关性	送检单位必须通过文档或其他方式对相应的防护措施及其有效性进行描述和说明	防护措施的有效性必须通过检测	送检单位必须通过文档或其他方式对相应的防护措施及其有效性进行证明
2770	多项选择题	GM/T 0008《安全芯片密码检测准则》中，下列内容属于安全等级3的安全芯片对电磁分析攻击的要求的是（ ）。	安全芯片须具有相应措施保证算法运算时电磁辐射特征与密钥和敏感信息之间没有明显的相关性	送检单位必须通过文档或其他方式对相应的防护措施及其有效性进行描述和说明	防护措施的有效性必须通过检测	送检单位必须通过文档或其他方式对相应的防护措施及其有效性进行证明
2771	判断题	GM/T 0008《安全芯片密码检测准则》中，无论哪一级别的安全芯片，其源文件都必须安全存放。	正确	错误		

2772	判断题	GM/T 0008《安全芯片密码检测准则》中，安全芯片中的固件可以允许通过接口读出 。	正确	错误		
2773	判断题	GM/T 0008《安全芯片密码检测准则》中，达到安全等级1的安全芯片要求须支持敏感信息以密文形式存储。	正确	错误		
2774	判断题	GM/T 0008《安全芯片密码检测准则》中，达到安全等级1的安全芯片要求须具有以硬件实现的对敏感信息的访问控制机制。	正确	错误		
2775	判断题	GM/T 0008《安全芯片密码检测准则》中，达到安全等级1的安全芯片对计时攻击无要求。	正确	错误		
2776	判断题	GM/T 0008《安全芯片密码检测准则》中，安全芯片支持的物理接口中可以含有隐式通道。	正确	错误		
2777	判断题	GM/T 0008《安全芯片密码检测准则》中，安全芯片支持的各种不同物理接口输入输出的密码算法的运算数据须一致。	正确	错误		
2778	判断题	GM/T 0008《安全芯片密码检测准则》中，达到安全等级1级的安全芯片可应用于安全芯片所部署的外部运行环境能够保障安全芯片自身物理安全和输入输出信息安全的应用场合。	正确	错误		
2779	单项选择题	GM/T 0008《安全芯片密码检测准则》中，规定的芯片安全能力共有（）个级别。	1	2	3	4
2780	单项选择题	GM/T 0008《安全芯片密码检测准则》中，下列内容不属于安全等级2对密钥存储的要求的是（）。	能够正确有效的存储密钥	支持带校验的密钥存储	存储的密钥以及密钥相关信息存放在可控且专用的存储区域	安全芯片须支持以密文形式存储密钥

2781	多项选择题	GM/T 0008《安全芯片密码检测准则》中，下列内容属于安全等级2对故障攻击的要求的是（）。	当安全芯片工作条件中的电压、频率、温度等可导致故障的工作参数的改变使安全芯片处于易受攻击状态时，安全芯片应能够发现这些工作条件的改变，并采取相应的防护措施保护密钥和敏感信息不泄露	送检单位必须通过文档或其他方式对相应的防护措施及其有效性进行描述和说明	防护措施的有效性必须通过检测	安全芯片须具有对光攻击的抵抗能力，并能够采取相应的防护措施保护密钥和敏感信息不泄露。
2782	单项选择题	根据GM/T 0035.2《射频识别系统密码应用技术要求第2部分：电子标签芯片密码应用技术要求》，完整性是电子标签的密码安全要素之一，其中存储信息完整性保护应采用密码算法，通过对存储的数据加（）的方式进行。	条形码	校验码	循环码	二维码
2783	单项选择题	根据GM/T 0035.2《射频识别系统密码应用技术要求第2部分：电子标签芯片密码应用技术要求》，唯一标识符鉴别需要在电子标签中存储（）以及验证码（MAC）。	UID	PID	CID	VID
2784	单项选择题	根据GM/T 0035.2《射频识别系统密码应用技术要求第2部分：电子标签芯片密码应用技术要求》，下列选项中不属于电子标签的身份鉴别方法的是（）。	唯一性标识符鉴别	电子标签对读写器的挑战响应鉴别	读写器对电子标签的挑战响应鉴别	读写器对读写器的挑战响应鉴别
2785	单项选择题	GM/T 0035.2《射频识别系统密码应用技术要求第2部分：电子标签芯片密码应用技术要求》附录A中示例的电子标签芯片所使用的SM7算法是一种（）算法。	消息鉴别码	非对称	密码杂凑	对称

2786	单项选择题	根据GM/T 0035.2《射频识别系统密码应用技术要求第2部分：电子标签芯片密码应用技术要求》，支持抗电子标签抵赖时，电子标签应具有（）功能。	产生数字签名	对读写器产生的数字签名进行验证的	加密	解密
2787	单项选择题	根据GM/T 0035.2《射频识别系统密码应用技术要求第2部分：电子标签芯片密码应用技术要求》，电子标签存储信息的机密性保护应采用密码算法（）完成。	加密	解密	签名	验签
2788	多项选择题	根据GM/T 0035.2《射频识别系统密码应用技术要求第2部分：电子标签芯片密码应用技术要求》，抗抵赖是电子标签密码安全要素之一，它包括（）。	抗通信系统抵赖	抗电子标签抵赖	抗读写器抵赖	抗电子标签原发抵赖
2789	多项选择题	根据GM/T 0035.2《射频识别系统密码应用技术要求第2部分：电子标签芯片密码应用技术要求》，电子标签的密码安全要素包括（）、身份鉴别、访问控制、审计记录、密码配置和其它安全措施。	机密性	完整性	防冲突	抗抵赖
2790	多项选择题	根据GM/T 0035.2《射频识别系统密码应用技术要求第2部分：电子标签芯片密码应用技术要求》，电子标签采用密码算法对存储在电子标签内的敏感信息进行校验计算，以发现数据（）等情况，确保存储数据的完整性。	篡改	删除	插入	复制
2791	多项选择题	根据GM/T 0035.2《射频识别系统密码应用技术要求第2部分：电子标签芯片密码应用技术要求》，电子标签的机密性保护须通过对传输的明文数据进行加密完成，可采用下列方式方式中的（）进行。	流加密	非对称加密	分组加密	杂凑

2792	多项选择题	根据GM/T 0035.2《射频识别系统密码应用技术要求第2部分：电子标签芯片密码应用技术要求》，电子标签在设计时除了要考虑机密性，完整性，审计记录等安全密码要素外，还要考虑其他安全措施，如（ ）等。	抗功耗分析	抗电磁分析	抗故障分析	抗物理攻击
2793	多项选择题	根据GM/T 0035.2《射频识别系统密码应用技术要求第2部分：电子标签芯片密码应用技术要求》，下列选项中属于电子标签的密钥管理的是（ ）。	密钥注入	密钥存储	密钥使用	密钥导出
2794	判断题	根据GM/T 0035.2《射频识别系统密码应用技术要求第2部分：电子标签芯片密码应用技术要求》，电子标签对存储在电子标签内的敏感信息采用密码算法进行加密保护，确保除合法读写器外，其余任何读写器不能获得该数据。	正确	错误		
2795	判断题	根据GM/T 0035.2《射频识别系统密码应用技术要求第2部分：电子标签芯片密码应用技术要求》，电子标签采用非对称密码算法产生的数字签名可用于数据完整性校验。	正确	错误		
2796	判断题	根据GM/T 0035.2《射频识别系统密码应用技术要求第2部分：电子标签芯片密码应用技术要求》，验证码(MAC)是由UID与相关应用信息关联后采用密码算法计算产生，并在发行电子标签时写入。	正确	错误		
2797	判断题	根据GM/T 0035.2《射频识别系统密码应用技术要求第2部分：电子标签芯片密码应用技术要求》，标识类电子标签不具备密码技术保护功能，可用于物流跟踪和物品识别等应用。	正确	错误		

2798	判断题	根据GM/T 0035.2《射频识别系统密码应用技术要求第2部分：电子标签芯片密码应用技术要求》，电子门票中所用电子标签属于防伪类电子标签。	正确	错误		
2799	单项选择题	根据GM/T 0035.3《射频识别系统密码应用技术要求第3部分：读写器密码应用技术要求》，电子标签对读写器的身份鉴别出现在安全级别（ ）以上。	1	2	3	4
2800	单项选择题	根据GM/T 0035.4《射频识别系统密码应用技术要求第4部分：电子标签与读写器通信密码应用技术要求》，双向鉴别前，读写器系统通过UID获得电子标签芯片的（ ）。	根密钥	分散密钥	分散因子	标签数据
2801	单项选择题	根据GM/T 0035.5《射频识别系统密码应用技术要求第5部分：密钥管理技术要求》，射频识别系统中的密钥体制包括（ ）类。	2	3	4	5
2802	单项选择题	根据GM/T 0035.5《射频识别系统密码应用技术要求第5部分：密钥管理技术要求》，对称密钥体制中密钥类别包括（ ）类。	1	2	3	4
2803	单项选择题	根据GM/T 0035.5《射频识别系统密码应用技术要求第5部分：密钥管理技术要求》，标签存储的的分散密钥由根密钥和（ ）通过密码算法生成。	根密钥	分散密钥	分散因子	标签
2804	单项选择题	根据GM/T 0035.5《射频识别系统密码应用技术要求第5部分：密钥管理技术要求》，分散因子长度不小于（ ）。	2字节	4字节	8字节	16字节
2805	单项选择题	根据GM/T 0035.5《射频识别系统密码应用技术要求第5部分：密钥管理技术要求》，标签密钥不可以被（ ）。	注入	使用	注销	读出

2806	单项选择题	根据GM/T 0035.5《射频识别系统密码应用技术要求第5部分：密钥管理技术要求》，哪个不属于密钥管理范围（ ）。	生成	分发	注入	混淆
2807	单项选择题	GM/T 0107《智能IC卡密钥管理系统基本技术要求》中，（ ）负责生成和管理根公钥和根私钥，并自签根公钥证书，同时为发卡机构签发发卡机构公钥证书。	根密钥管理系统	发卡机构密钥管理系统	发卡机构的智能IC卡密钥管理系统	以上都是
2808	单项选择题	GM/T 0107《智能IC卡密钥管理系统基本技术要求》中，（ ）生成发卡机构的公私钥对，并提交相应的公钥请求文件由根密钥管理系统签发发卡机构公钥证书；同时生成和管理具体的IC卡公私钥对，并签发IC卡公钥证书。	根密钥管理系统	发卡机构密钥管理系统	发卡机构的智能IC卡密钥管理系统	以上都是
2809	单项选择题	GM/T 0107《智能IC卡密钥管理系统基本技术要求》中，（ ）负责生成和管理IC卡业务根密钥和根公钥证书，并签发下级机构证书或者分散生成下级机构业务密钥。	IC卡清结算系统	IC卡卡管系统	发卡机构侧的智能IC卡密钥管理系统	上级机构侧的根密钥管理系统
2810	单项选择题	GM/T 0107《智能IC卡密钥管理系统基本技术要求》中，（ ）负责从上级机构导入证书和密钥，生成和管理本级机构的IC卡应用密钥和机构证书，并为IC卡发卡和交易提供密钥服务。	IC卡清结算系统	IC卡卡管系统	发卡机构侧的智能IC卡密钥管理系统	上级机构侧的根密钥管理系统
2811	单项选择题	GM/T 0107《智能IC卡密钥管理系统基本技术要求》那中，（ ）负责管理IC卡业务数据及为IC卡发卡和交易提供服务的系统，IC卡卡管系统部署IC卡交易类密钥（电子钱包类密钥或者电子现金密钥），通过这些密钥完成与IC卡的联机认证。	IC卡清结算系统	IC卡卡管系统	发卡机构侧的智能IC卡密钥管理系统	上级机构侧的根密钥管理系统

2812	单项选择题	GM/T 0107《智能IC卡密钥管理系统基本技术要求》中，下列属于发卡机构公私钥对功能的是（）。	用于脱机数据认证，根私钥用于自签根公钥证书，并为发卡机构签发发卡机构公钥证书，根公钥用于验证自签根公钥证书和发卡机构公钥证书	用于脱机数据认证，发卡机构私钥用于签发IC卡公钥证书，发卡机构公钥用于验证IC卡公钥证书	用于脱机数据认证，基于IC卡公私钥对完成交易数据的签名和认证	用于产生IC卡应用开通密钥，用于与扩展应用相关的安全应用开通密钥报文鉴别码的产生和验证
2813	单项选择题	GM/T 0107《智能IC卡密钥管理系统基本技术要求》中，（）用于产生和管理部分业务根密钥，并分散产生发卡机构业务根密钥。	发卡机构根密钥管理系统	IC卡卡管系统	发卡机构侧的智能IC卡密钥管理系统	上级机构侧的根密钥管理系统
2814	单项选择题	GM/T 0107《智能IC卡密钥管理系统基本技术要求》中，智能IC卡管理类密钥不包含下列密钥中的（）。	根公私钥对	应用维护主密钥	应用开通主密钥	卡片维护主密钥
2815	单项选择题	GM/T 0107《智能IC卡密钥管理系统基本技术要求》中，IC卡业务密钥的对称密钥体系一般都是多级分散结构的，根密钥管理系统产生和管理部分业务根密钥并分散产生（）。	IC卡密钥	发卡机构业务根密钥	应用开通主密钥	卡片维护主密钥
2816	单项选择题	GM/T 0107《智能IC卡密钥管理系统基本技术要求》中，发卡机构智能IC卡密钥管理系统导入上级机构产生的部分业务根密钥，并产生部分自己独立管理和维护的业务根密钥，再经过一级或者多级分散产生（）。	IC卡密钥	发卡机构业务根密钥	应用开通主密钥	卡片维护主密钥
2817	多项选择题	GM/T 0107《智能IC卡密钥管理系统基本技术要求》中，智能IC卡业务密钥中的对称密钥按照用途可分为（）。	管理类密钥	交易类密钥	发卡机构公钥	发卡机构私钥

2818	多项选择题	GM/T 0107《智能IC卡密钥管理系统基本技术要求》中，下列IC卡业务密钥属于交易类密钥的是（）。	发卡机构主密钥	安全报文认证(MAC)主密钥	安全报文加密主密钥	TAC主密钥
2819	多项选择题	GM/T 0107《智能IC卡密钥管理系统基本技术要求》中，下列IC卡业务密钥属于管理类密钥的是（）。	发卡机构主密钥	卡片主控主密钥	卡片维护主密钥	应用主控主密钥
2820	多项选择题	GM/T 0107《智能IC卡密钥管理系统基本技术要求》中，系统保护密钥又可分为（）。	发卡机构主密钥	卡片主控主密钥	系统传输保护密钥	系统存储保护密钥
2821	多项选择题	GM/T 0107《智能IC卡密钥管理系统基本技术要求》中，以下对已归档密钥的使用要求，说法正确的是（）。	已归档的密钥只能用于证明在归档前进行的交易的合法性	已归档的密钥不应返回到操作使用中	已归档密钥不能影响在用的密钥的安全	已归档的密钥可以重新恢复并加以使用
2822	多项选择题	GM/T 0107《智能IC卡密钥管理系统基本技术要求》中，关于非对称密钥的分发，以下说法正确的是（）。	发卡机构私钥仅存储在智能IC卡密钥管理系统中，无需进行分发	IC卡私钥应分发到数据准备系统及IC卡发卡系统中，分发过程应采用系统传输保护密钥加密后分发	发卡机构公钥证书和IC卡公钥证书可直接分发到数据准备系统及IC卡发卡系统中	发卡机构公私钥对应保存在密码模块中
2823	判断题	GM/T 0107《智能IC卡密钥管理系统基本技术要求》中，发卡机构公私钥对不再使用后，应进行密钥归档。	正确	错误		
2824	判断题	GM/T 0107《智能IC卡密钥管理系统基本技术要求》中，对过期或者已经泄露或者其他原因不再使用的非对称密钥无需进行销毁操作。	正确	错误		
2825	判断题	GM/T 0107《智能IC卡密钥管理系统基本技术要求》中，IC卡业务密钥可分为对称密钥和非对称密钥，对称密钥按照用途又可以划分为管理类密钥和交易类密钥两种类型。	正确	错误		

2826	判断题	GM/T 0107《智能IC卡密钥管理系统基本技术要求》中，IC卡业务密钥的对称密钥主要涉及管理类密钥和交易类密钥，主要作用是保证发卡过程和交易过程的安全。	正确	错误		
2827	单项选择题	在GM/T 0104《云服务器密码机技术规范》中，虚拟密码机的作用是（ ）。	为租户和应用提供密码服务	提供物理设备的处理器、网络、存储等资源	进行设备维护	执行虚拟密码机的创建、启动、关闭、删除、漂移等操作
2828	单项选择题	根据GM/T 0104《云服务器密码机技术规范》，云服务器密码机的宿主机和不同虚拟密码机的远程管理通道和维护通道应采用（ ）进行保护。	加密和身份鉴别等技术手段	虚拟化技术	网络技术	冗余备份技术
2829	单项选择题	根据GM/T 0104《云服务器密码机技术规范》，虚拟密码机可由（ ）进行集中统一管理。	云平台管理系统	虚拟密码机所属租户自己的管理系统	宿主机管理员	其他虚拟密码机的管理员
2830	单项选择题	根据GM/T 0104《云服务器密码机技术规范》，宿主机（ ）管理和访问虚拟密码机的密钥。	可以	不可以	只能管理，不能访问	只能访问，不能管理
2831	单项选择题	根据GM/T 0104《云服务器密码机技术规范》，云服务器密码机机必须至少支持（ ）密钥结构。	1层	2层	3层	4层
2832	单项选择题	根据GM/T 0104《云服务器密码机技术规范》，云服务器密码机的用户密钥包括（ ）。	签名密钥对和加密密钥对	签名密钥对和会话密钥对	加密密钥对和会话密钥对	只有一个密钥对
2833	判断题	根据GM/T 0104《云服务器密码机技术规范》，宿主机和不同虚拟密码机可采用基于硬件或软件的虚拟化技术进行隔离。	正确	错误		
2834	单项选择题	根据GM/T 0104《云服务器密码机技术规范》，云服务器密码机的随机数发生器应该至少采用（ ）个独立的物理噪声源芯片。	1	2	3	4

2835	单项选择题	根据GM/T 0104《云服务器密码机技术规范》，云服务器密码机中使用虚拟密码机的租户/应用和虚拟密码机之间的身份鉴别机制需要满足（ ）。	单向鉴别	双向鉴别	口令鉴别	OAUTH鉴别
2836	多项选择题	根据GM/T 0104《云服务器密码机技术规范》，下列选项属于虚拟密码机的日志内容的是（ ）。	管理员操作行为，包括登录认证、系统配置、密钥管理等操作	异常事件，包括认证失败、非法访问等异常事件的记录	硬件部件自检记录	物理网络检查记录
2837	多项选择题	根据GM/T 0104《云服务器密码机技术规范》，云服务器密码机宿主机和不同虚拟密码机应提供日志记录、查看和导出功能，日志的存储和操作应满足下列要求中的（ ）。	宿主机和不同虚拟密码机的日志记录应独立存储和操作	宿主机和不同虚拟密码机的日志记录仅能由宿主机和不同虚拟密码机自身的管理员访问	宜提供关键日志记录的完整性校验或其他防篡改功能	宿主机和不同虚拟密码机的管理员可以相互访问对方的日志记录
2838	单项选择题	GM/T 0104《云服务器密码机技术规范》中要求虚拟密码机的镜像文件应进行（ ）保护。	签名	加密	不可否认性	可信度
2839	多项选择题	根据GM/T 0104《云服务器密码机技术规范》，下列选项中属于云服务器密码机宿主机自检功能中包含的内容的是（ ）。	硬件部件自检	密码部件自检	虚拟化功能自检	所存储数据的完整性检查
2840	多项选择题	根据GM/T 0104《云服务器密码机技术规范》，关于云服务器密码机的虚拟密码机镜像安全，下列描述正确的是（ ）。	虚拟密码机的镜像文件应进行签名保护	云服务器密码机应禁止签名验证不通过的虚拟密码机镜像在云服务器密码机中运行	虚拟密码机的镜像文件无需进行签名保护	云服务器密码机不需要对虚拟密码机镜像进行验证
2841	多项选择题	GM/T 0104《云服务器密码机技术规范》中要求虚拟密码机应具备下列状态中的（ ）。	初始状态	就绪状态	关闭状态	挂起状态
2842	多项选择题	GM/T 0104《云服务器密码机技术规范》中要求云服务器密码机宿主机应具备下列状态中的（ ）。	初始状态	就绪状态	关闭状态	挂起状态

2843	多项选择题	GM/T 0104《云服务器密码机技术规范》中要求虚拟密码机应当至少支持下列密码算法中的（ ）。	SM1	SM2	SM3	SM4
2844	多项选择题	在GM/T 0104《云服务器密码机技术规范》中，规定虚拟密码机所支持的对称密码工作模式至少包括下列选项中的（ ）。	输出反馈OFB	电子密本ECB	分组密码链接CBC	密码反馈CFB
2845	多项选择题	根据GM/T 0104《云服务器密码机技术规范》，云服务器密码机中的虚拟密码机自检宜包括以下功能中的（ ）。	密码算法正确性检查	随机数发生器检查	虚拟网络检查	所存储密钥和数据的完整性检查
2846	多项选择题	根据GM/T 0104《云服务器密码机技术规范》，云服务密码机宿主机的初始化包括下列选项中的（ ）。	宿主机密钥的生成（恢复）与安装	生成管理员	按照安全机制对密钥进行安全存储和备份	生成数字证书
2847	多项选择题	GM/T 0104《云服务器密码机技术规范》的检测要求规定了云服务器密码机的通用检测内容和方法，检测应包括（ ）。	外观和结构检查	提交文档的检查	功能检测	性能检测
2848	多项选择题	GM/T 0104《云服务器密码机技术规范》规定设备的管理检测包括（ ）。	管理操作检测	管理登录检测	管理接口检测	日志审计检测
2849	多项选择题	虚拟密码机管理密钥的安全存储可采用以下方式（ ）。	采用授权码结合其他密钥分量（如随机数或硬件特征码等）进行加密存储	在具有微电保护和毁钥触发装置的密钥存储部件上存储	在智能密码钥匙等外置密码模块上存储	在运行日志中存储
2850	判断题	根据GM/T 0104《云服务器密码机技术规范》，宿主机可以管理和访问虚拟密码机的密钥。	正确	错误		
2851	判断题	根据GM/T 0104《云服务器密码机技术规范》，云服务器密码机的宿主机和虚拟密码机应具有启动时自检和接收自检指令时自检的功能。	正确	错误		
2852	判断题	根据GM/T 0104《云服务器密码机技术规范》，虚拟密码机的作用是执行虚拟密码机的创建、启动、关闭、删除、漂移等操作。	正确	错误		

2853	判断题	根据GM/T 0104《云服务器密码机技术规范》，虚拟密码机在初始状态下能提供密码服务。	正确	错误		
2854	判断题	根据GM/T 0104《云服务器密码机技术规范》，宿主机和不同虚拟密码机应该具有各自完全独立的管理密钥、设备密钥、用户密钥、密钥加密密钥和会话密钥。	正确	错误		
2855	判断题	根据GM/T 0104《云服务器密码机技术规范》，云服务器密码机的宿主机和虚拟密码机的日志记录应该独立存储和操作。	正确	错误		
2856	判断题	根据GM/T 0104《云服务器密码机技术规范》，云服务器密码机在逻辑上由一个宿主机和若干个虚拟密码机组成，其中宿主机不向应用提供密码服务。	正确	错误		
2857	判断题	根据GM/T 0104《云服务器密码机技术规范》，云服务器密码机的宿主机和不同虚拟密码机的远程管理通道和维护通道彼应相互独立。	正确	错误		
2858	判断题	根据GM/T 0104《云服务器密码机技术规范》，虚拟密码机和租户可以访问宿主机的管理密钥。	正确	错误		
2859	判断题	根据GM/T 0104《云服务器密码机技术规范》，云服务器密码机中设备密钥的使用对租户和应用开放。	正确	错误		
2860	判断题	根据GM/T 0104《云服务器密码机技术规范》，宿主机的管理员和维护人员可以登录虚拟密码机，获取信息和访问服务。	正确	错误		
2861	单项选择题	GM/T 0088《云服务器密码机管理接口规范》中，云服务器密码机CHSM数据影像包含CHSM内所有VSM中的与用户相关的配置、密钥及敏感信息等，主要用于（）过程。	CHSM备份	VSM漂移	VSM重置	CHSM漂移

2862	单项选择题	GM/T 0088《云服务器密码机管理接口规范》中，虚拟密码机VSM数据影像包含与用户相关的配置、密钥及敏感信息等，主要用于（ ）过程。	云服务器密码机备份CHSM	VSM漂移	VSM重置	VSM升级
2863	单项选择题	GM/T 0088《云服务器密码机管理接口规范》中，定义了（ ）之间的通讯协议。	云平台管理系统和云服务器密码机	租户与云服务器密码机	租户与VSM	云服务器密码机与VSM
2864	单项选择题	根据GM/T 0088《云服务器密码机管理接口规范》，云服务器密码机管理接口API被（ ）调用。	云服务器密码机	租户	云平台管理系统	业务系统
2865	单项选择题	根据GM/T 0088《云服务器密码机管理接口规范》，云服务器密码机管理接口API，认证信息包含在http请求的（ ）中。	Body	Url	Header	Script
2866	多项选择题	根据GM/T 0088《云服务器密码机管理接口规范》，云服务器密码机管理接口API用于管理（ ）。	云服务器密码机CHSM	KVM	虚拟密码机VSM	API
2867	多项选择题	GM/T 0088《云服务器密码机管理接口规范》中规定云服务器密码机管理接口API可以使用下列通信协议中的（ ）。	HTTP	TCP	UDP	TLCP协议
2868	多项选择题	根据GM/T 0088《云服务器密码机管理接口规范》，云服务器密码机管理接口API，定义的接口采用的http请求方法包括（ ）。	PUT	GET	HEAD	POST
2869	多项选择题	根据GM/T 0088《云服务器密码机管理接口规范》，云服务器密码机管理接口API，在http请求的header中包含的认证信息，包含下列域中的（ ）。	CHSM-AuthPK	CHSM-SignatureAlg	CHSM-Signature	CHSM-Id
2870	多项选择题	根据GM/T 0088《云服务器密码机管理接口规范》，云服务器密码机管理接口API中，可获取的虚拟密码机VSM的状态包括下列选项中的（ ）。	就绪状态normal	初始状态initial	错误状态error	关机状态shutdown

2871	多项选择题	根据GM/T 0088《云服务器密码机管理接口规范》，云服务器密码机管理接口API中，每个接口的输出中都返回的参数包括下列选项中的（ ）。	requestId请求ID	status状态码	message状态描述	timestamp服务器响应时间
2872	多项选择题	根据GM/T 0088《云服务器密码机管理接口规范》，允许通过调用云服务器密码机管理接口API，对VSM进行以下那种操作（ ）。	创建/删除	启动/停止	重启	重置
2873	判断题	根据GM/T 0088《云服务器密码机管理接口规范》，每个虚拟密码机VSM都有唯一的UUID来标识。	正确	错误		
2874	判断题	根据GM/T 0088《云服务器密码机管理接口规范》，云服务器密码机管理接口API，由云平台管理系统调用。	正确	错误		
2875	判断题	云根据GM/T 0088《云服务器密码机管理接口规范》，服务器密码机管理接口API，在http请求的header中包含认证信息。	正确	错误		
2876	判断题	根据GM/T 0088《云服务器密码机管理接口规范》，云服务器密码机管理接口API，要求每个http请求必须返回状态信息。	正确	错误		
2877	判断题	根据GM/T 0088《云服务器密码机管理接口规范》，云服务器密码机的NTP（网络时间协议）服务器地址能够通过云服务器密码机管理接口API进行设置。	正确	错误		
2878	单项选择题	GM/T 0103《随机数发生器总体框架》中，熵源通过对部件、设备或者事件中的不确定性进行采样量化，得到（ ）。	随机源序列	模拟序列	后处理序列	信号系统

2879	单项选择题	GM/T 0103《随机数发生器总体框架》中，随机数发生器通常包括设计、产品检测以及使用阶段，在（ ）对熵源或随机源序列进行熵评估。	产品检测阶段	设计阶段	产品检测及使用阶段	使用阶段
2880	单项选择题	GM/T 0103《随机数发生器总体框架》中，随机数发生器通常包括设计、产品检测以及使用阶段，在（ ）对随机源序列或随机数序列进行有效性检验或随机性检验。	产品检测阶段	设计阶段	产品检测及使用阶段	使用阶段
2881	单项选择题	GM/T 0103《随机数发生器总体框架》中，随机数发生器产生随机数过程中，（ ）是由时域不稳定性引起的波相位的快速、短期且具有随机特性的波动。	相位抖动	时钟抖动	随机抖动	峰值抖动
2882	单项选择题	GM/T 0103《随机数发生器总体框架》中，物理熵源输出的熵应当可以被从理论上估计，并且估计值要（ ）一定的阈值。	等于	大于	小于	大于等于
2883	单项选择题	GM/T 0103《随机数发生器总体框架》中，量子随机过程是具有（ ）的随机现象/过程。	量子测不准	量子噪声	内秉量子随机性	量子涨落
2884	单项选择题	GM/T 0103《随机数发生器总体框架》中，（ ）是在元器件中，通常情况下不希望出现的，但却内在产生的杂散电子信号。	辐射噪声	量化噪声	传导噪声	热噪声
2885	单项选择题	GM/T 0103《随机数发生器总体框架》中，（ ）是随机数发生器产生随机数的来源。	熵源	后处理	数字采样	熵评估
2886	单项选择题	GM/T 0103《随机数发生器总体框架》中，熵源是产生输出的部件、设备或事件。当该输出以某种方法捕获和处理时，产生（ ）。	后处理比特串	包含熵的比特串	确定性比特串	可预测比特串
2887	单项选择题	GM/T 0103《随机数发生器总体框架》中，非物理熵源由（ ）提供。	存储器	CPU	代码程序	随机数发生器所在的运行环境

2888	单项选择题	GM/T 0103《随机数发生器总体框架》中，下列随机数发生器后处理算法中属于轻量级后处理方法的是（ ）。	序列密码算法	冯·诺依曼校正器	分组密码算法	杂凑函数
2889	单项选择题	GM/T 0103《随机数发生器总体框架》中，下列随机数发生器后处理算法中不属于密码函数后处理方法的是（ ）。	AES算法	杂凑函数	m-LSB	SM4算法
2890	多项选择题	GM/T 0103《随机数发生器总体框架》中，熵源常用的设计原理包括（ ）。	相位抖动原理	热噪声直接放大原理	混沌振荡原理	量子随机过程和其他随机事件等
2891	多项选择题	GM/T 0103《随机数发生器总体框架》中，熵源分为（ ）。	物理熵源	非物理熵源	数字熵源	模拟熵源
2892	多项选择题	GM/T 0103《随机数发生器总体框架》中，用于产生随机数的量子随机过程一般包括（ ）。	单光子路径选择	相邻光子间时间间隔	激光相位噪声	放大自发辐射噪声
2893	多项选择题	GM/T 0103《随机数发生器总体框架》中，随机数发生器检测模块对随机源序列或随机数序列进行（ ），以保证随机数发生器的功能正确性及质量安全性。	失效检验	稳定性检验	随机性检验	安全性检验
2894	多项选择题	GM/T 0103《随机数发生器总体框架》中，随机数发生器后处理算法有很多，其中密码函数后处理方法包括（ ）等。	基于分组密码	基于杂凑函数	基于公钥密码	基于m序列
2895	单项选择题	GM/T 0103《随机数发生器总体框架》中，随机数发生器后处理算法有很多，其中密码函数后处理方法不包括（ ）。	基于分组密码	基于杂凑函数	基于公钥密码	基于m序列
2896	判断题	GM/T 0103《随机数发生器总体框架》中，随机数发生器熵源通过对部件、设备或者事件中的不确定性进行采样量化，得到随机源序列。	正确	错误		
2897	判断题	GM/T 0103《随机数发生器总体框架》中，热噪声又称“相位抖动噪声”	正确	错误		

2898	判断题	GM/T 0103《随机数发生器总体框架》中，随机数发生器的后处理模块是可选的，实际应用中应保证后处理的功能正确性。	正确	错误		
2899	判断题	GM/T 0103《随机数发生器总体框架》中，随机数发生器的熵评估必须在随机数发生器内部实现。	正确	错误		
2900	判断题	GM/T 0103《随机数发生器总体框架》中，随机数发生器的检测模块检测失败时，应根据检测输出做出相应处理，如产生报警信号等。	正确	错误		
2901	判断题	GM/T 0103《随机数发生器总体框架》中，随机数发生器的后处理模块是可选的，实际中应根据随机源序列的统计特性决定是否选用。	正确	错误		
2902	单项选择题	GM/T 0105《软件随机数发生器设计指南》以（）比特的最小熵值为基准来给出软件随机数发生器的参数信息。	8	32	256	2048
2903	单项选择题	GM/T 0105《软件随机数发生器设计指南》定义软件随机数发生器是软件密码模块或（）中的随机数发生器部件。	混合密码模块的软件部件	硬件密码模块的软件部件	固件密码模块的软件部件	特定密码模块的软件部件
2904	单项选择题	GM/T 0105《软件随机数发生器设计指南》中规定的软件随机数发生器基本模型不包括以下哪个（）部件。	熵池	重启函数	DRNG	健康测试
2905	单项选择题	GM/T 0105《软件随机数发生器设计指南》中建议熵池大小应大于等于（）字节，但不宜超过（）字节。	5,001,024	1024、4096	512、4096	256、4096
2906	单项选择题	根据GM/T 0105《软件随机数发生器设计指南》，以下哪项（）不属于确定性随机数发生器DRNG的组成部分。	初始化函数	重播种函数	输出函数	熵池

2907	单项选择题	为了保障软件随机数发生器的可靠性，GM/T 0105《软件随机数发生器设计指南》建议随机性来源不少于（ ）种。	2	3	4	5
2908	单项选择题	根据GM/T 0105《软件随机数发生器设计指南》，下列哪项（ ）不属于通用操作系统上随机性来源。	系统中断事件	鼠标位移	系统时间	CPU内置硬件随机数发生器
2909	单项选择题	关于GM/T 0105《软件随机数发生器设计指南》中熵估计的说法，不正确的是（ ）。	为保证随机数实时产出的质量，熵估计模块需要嵌入软件随机数发生器内部	熵估计采用的是数学算法来计算的	熵估计是对最小熵的评估	熵估计的对象是熵源的输出，而非软件随机数发生器最终的输出
2910	单项选择题	根据GM/T 0105《软件随机数发生器设计指南》对DRNG输入的nonce要求和描述，不正确的是（ ）。	当软件RNG的熵源存在故障时，nonce能够在一定程度上提供额外安全保障	nonce应至少具有128比特熵	时间戳不可以作为nonce	nonce作为DRNG必选输入
2911	单项选择题	关于GM/T 0105《软件随机数发生器设计指南》中的说法，不正确的是（ ）。	熵池大小应不小于512字节	扩展函数中，仅使用密码杂凑算法可保证压缩结果的熵是不充足的	对安全级别二级的密码模块，当距离上一次重播种时间间隔超过60s时需要执行重播种操作	健康测试用于监测熵源和DRNG的状态
2912	单项选择题	GM/T 0105《软件随机数发生器设计指南》中规定，基于SM3算法和基于SM4算法的RNG设计中生成的种子的长度分别为（ ）比特。	440,256	256、256	128、256	440、128
2913	多项选择题	GM/T 0105《软件随机数发生器设计指南》对于安全二级和安全一级的密码模块，主要区别在于（ ）。	DRNG重播种时间间隔	输出函数被调用次数	是否包含健康测试	涉及到的熵源数量
2914	多项选择题	以下属于GM/T 0105《软件随机数发生器设计指南》列举的通用熵源类型的是（ ）。	系统时间	特定的系统中断事件	磁盘状态	人机交互输入事件

2915	多项选择题	下列选项中可以作为GM/T 0105《软件随机数发生器设计指南》中提及的个性化字符串的是（）。	设备序列号	公钥信息	用户标识	网络地址
2916	多项选择题	根据GM/T 0105《软件随机数发生器设计指南》，针对GB/T 37092《信息安全技术 密码模块安全要求》安全等级二级，以下哪些情况需要对DRNG执行重播种操作（）。	距离上一次DRNG重播种时间超过了600秒	输出函数已被调用2^20次	距离上一次DRNG重播种时间超过了60秒	输出函数已被调用2^10次
2917	多项选择题	GM/T 0105《软件随机数发生器设计指南》中建议，除熵输入外，DRNG输入还可以包括（）	个性化字符串	额外输入	nonce	设备序列号
2918	多项选择题	GM/T 0105《软件随机数发生器设计指南》规定了基于（）密码算法的确定性随机数发生器（DRNG）。	SM3	SM2	SM9	SM4
2919	多项选择题	根据GM/T 0105《软件随机数发生器设计指南》，以下哪种（）健康测试是必须要做的。	上电健康测试	连续健康测试	周期测试	按需健康测试
2920	多项选择题	GM/T 0105《软件随机数发生器设计指南》规定的健康测试包括（）。	随意健康测试	连续健康测试	按需健康测试	上电健康测试
2921	多项选择题	GM/T 0105《软件随机数发生器设计指南》规定的关键安全参数包括（）。	熵源产生的熵	DRNG内部状态中的敏感状态信息	DRNG熵输入	DRNG中重播种计数器阈值
2922	多项选择题	GM/T 0105《软件随机数发生器设计指南》中建议，可以通过以下哪些机制保证熵源的独占性（）。	在同一运行环境下，熵源可以被多个应用程序同时访问	熵源同一时刻只能为一个实例提供熵，当熵源被占用时，将拒绝其他实体的访问	操作系统通过互斥锁的机制，保证只有一个实体可以访问该熵源	软件随机数发生器自身的机制保证熵源访问的独占性
2923	判断题	GM/T 0105《软件随机数发生器设计指南》对于安全二级和安全一级的密码模块中的软件随机数发生器只在重播种时机上有区别，其他方面的要求是一致的。	正确	错误		

2924	判断题	按照GM/T 0105《软件随机数发生器设计指南》建议，当选用基于SM4算法的DRNG实例时，DRNG输出一组随机数据的长度为256比特。	正确	错误		
2925	判断题	按照GM/T 0105《软件随机数发生器设计指南》建议，当选用基于SM3算法的DRNG实例时，DRNG输出一组随机数据的长度为256比特。	正确	错误		
2926	判断题	根据GM/T 0105《软件随机数发生器设计指南》中说明，DRNG自身安全性依赖于nonce和个性化字符串的保密性。	正确	错误		
2927	判断题	对于GM/T 0105《软件随机数发生器设计指南》中规定的熵源，系统随机数发生器和硬件随机数发生器是可选的，系统熵源是必选的。	正确	错误		
2928	判断题	按照GM/T 0105《软件随机数发生器设计指南》，软件随机数发生器和其他密码模块一样，也分为安全等级一级、二级、三级、四级。	正确	错误		
2929	判断题	按照GM/T 0105《软件随机数发生器设计指南》，对DRNG的自测试可以作为其所在软件密码模块自测试的一部分，也可以单独执行。	正确	错误		
2930	判断题	根据GM/T 0105《软件随机数发生器设计指南》要求熵源同一时刻只能被一个软件随机数发生器独占访问，以保证软件随机数发生器独占过程中所读取的熵源数据无法被其他实体获取。	正确	错误		
2931	判断题	GM/T 0105《软件随机数发生器设计指南》中规定，重播种计数器阈值和重播种时间阈值与安全等级有关，不同安全等级的软件随机数发生器，重播种计数器阈值和重播种时间阈值有所不同。	正确	错误		

2932	多项选择题	在GM/T 0062《密码产品随机数检测要求》中关于随机数检测的不同产品形态类别主要特征描述正确的是（）。	A类产品不能独立作为功能产品使用	B类产品用时上电，随机数检测处理能力有限，对上电响应速度有严格要求	C类产品用时上电，随机数检测处理能力有限，对上电响应速度没有严格要求	D类产品长期加电，随机数检测处理能力有限，对上电响应速度没有严格要求
2933	单项选择题	GM/T 0062《密码产品随机数检测要求》将随机数检测划分为五个不同产品形态类别，其中A类产品不能独立作为功能产品使用，其典型产品形态为（）。	随机数发生器芯片	智能IC卡	智能密码钥匙	服务器密码机
2934	单项选择题	GM/T 0062《密码产品随机数检测要求》将随机数检测划分为五个不同产品形态类别，其中B类产品用时上电，随机数检测处理能力有限，对上电响应速度有严格要求，其典型产品形态为（）。	随机数发生器芯片	智能IC卡	POS机	云服务器密码机
2935	单项选择题	GM/T 0062《密码产品随机数检测要求》将随机数检测划分为五个不同产品形态类别，其中C类产品用时上电，随机数检测处理能力有限，对上电响应速度没有严格要求，其典型产品形态为（）。	随机数发生器芯片	电子标签	智能密码钥匙	SSL VPN网关
2936	单项选择题	GM/T 0062《密码产品随机数检测要求》将随机数检测划分为五个不同产品形态类别，其中D类产品长期加电，随机数检测处理能力有限，对上电响应速度没有严格要求，典型产品形态为（）。	USB接口芯片	智能IC卡	POS机	时间戳服务器
2937	单项选择题	GM/T 0062《密码产品随机数检测要求》将随机数检测划分为五个不同产品形态类别，其中E类产品长期加电，具有较强的随机数处理能力，对上电响应速度没有要求，其典型产品形态为（）。	随机数发生器芯片	智能IC卡	POS机	服务器密码机

2938	判断题	在GM/T 0062《密码产品随机数检测要求》中，送样检测是由厂家在产品出厂前自行进行的产品随机数功能和质量检测。	正确	错误		
2939	判断题	在GM/T 0062《密码产品随机数检测要求》中，周期检测是产品工作过程中按照一定的时间间隔自动进行的随机数功能检测。	正确	错误		
2940	单项选择题	在GM/T 0062《密码产品随机数检测要求》中，对（ ）的随机数使用检测没有要求。	A类产品	B类产品	C类产品	D类产品
2941	多项选择题	在GM/T 0062《密码产品随机数检测要求》中，（ ）需要对随机数进行周期检测。	B类产品	C类产品	D类产品	E类产品
2942	单项选择题	根据GM/T 0078《密码随机数生成模块设计指南》，关于随机数生成模块的一般模型以下说法错误的是（ ）。	物理随机源电路利用电路中物理过程的不确定性，并对物理过程中的不确定性进行采样量化，得到随机源序列	只有通过物理随机源检测的随机数序列才可以输出	后处理电路利用一定算法生成符合统计检验的随机数序列	随机数生成模块不提供随机数序列输出
2943	单项选择题	根据GM/T 0078《密码随机数生成模块设计指南》，随机数生成模块的一般模型不包括下列选项中的（ ）。	物理随机源电路	物理随机源失效检测电路	DRBG电路	后处理电路
2944	单项选择题	根据GM/T 0078《密码随机数生成模块设计指南》，对基于混沌原理的物理随机源，以下说法错误的是（ ）。	将随机性噪声作为混沌系统的微小扰动，由于系统的输出受系统中随机噪声的影响，使系统输出序列不可预测，产生随机序列	基于混沌动力系统原理实现物理随机源，主要考虑混沌函数的电路实现和随机噪声的实现	混沌系统包括离散混沌和连续混沌两种	采样频率需要足够快，保证采到足够多的迭代值

2945	单项选择题	根据GM/T 0078《密码随机数生成模块设计指南》，典型的基于相位抖动原理产生物理随机源模型不包括下列选项中的（）。	振荡源	采样时钟	比较器	触发器
2946	单项选择题	根据GM/T 0078《密码随机数生成模块设计指南》，在利用相位抖动原理实现的物理随机源电路设计中，下列操作中不能提高抗干扰能力的是（）。	在物理随机源电路的供电端加入稳压电路	在物理随机源电路的供电端加入滤波电路	加大电源随机干扰，提高随机性	改进振荡器的结构
2947	单项选择题	根据GM/T 0078《密码随机数生成模块设计指南》，对基于热噪声直接放大原理的物理随机源，以下说法错误的是（）。	热噪声是一个连续时间的随机白噪声，在给定频率带宽范围内，具有均匀噪声谱密度的白噪声其输出幅值呈正态分布	在任意给定的时间内，噪声电压值高于或低于平均值的概率呈线性关系	电阻的热噪声越大，噪声的带宽越宽，产生的随机数质量越好	电阻产生的热噪声幅度，需要满足该噪声经过放大器放大后能够被比较器所识别
2948	单项选择题	根据GM/T 0078《密码随机数生成模块设计指南》，典型的基于热噪声直接放大原理的物理随机源的模型不包括下列选项中的（）。	反馈电路	噪声源	噪声放大器	比较器
2949	单项选择题	GM/T 0078《密码随机数生成模块设计指南》中，使用分组密码算法作为后处理算法，其输入不包括下列选项中的（）。	密钥数据	初始向量	明文/密文数据	摘要
2950	单项选择题	GM/T 0078《密码随机数生成模块设计指南》中，密码函数方法的后处理算法不包括下列选项中的（）。	基于分组密码的后处理算法	基于杂凑函数的后处理算法	基于零知识证明的方法	基于m序列的后处理算法
2951	单项选择题	GM/T 0078《密码随机数生成模块设计指南》中，对（）进行检测能够检测到物理随机源失效。	物理随机源输出序列	后处理输出序列	随机数模块输出序列	伪随机序列
2952	单项选择题	GM/T 0078《密码随机数生成模块设计指南》中，检测到物理源失效后，下列措施不正确的是（）。	产生报警信号	停止输出随机数	清除缓存中的随机数	继续输出随机数

2953	多项选择题	根据GM/T 0078《密码随机数生成模块设计指南》，基于相位抖原理的物理随机源的输出的随机比特序列质量受（ ）的影响。	采样时钟的频率	振荡源输出信号的抖动的标准差	振荡源的振荡时钟频率	采样时钟信号的抖动的标准差
2954	多项选择题	根据GM/T 0078《密码随机数生成模块设计指南》，典型的基于混沌原理的物理随机源模型包括下列选项中的（ ）。	内部状态电路	反馈电路	采样电路	振荡源电路
2955	多项选择题	根据GM/T 0078《密码随机数生成模块设计指南》，基于相位抖动原理的物理随机源，主要包括下列方式中的（ ）。	快速时钟信号采样带抖动慢速振荡信号	带抖动快速的时钟信号采样慢速振荡信号	慢速时钟信号采样带抖动快速振荡信号	带抖动慢速的时钟信号采样快速振荡信号
2956	判断题	GM/T 0078《密码随机数生成模块设计指南》中，合成的多路物理随机源可以采用相同原理，也可以采用不同原理。	对	错误		
2957	判断题	GM/T 0078《密码随机数生成模块设计指南》中，每一路物理随机源电路是独立的。	对	错误		
2958	多项选择题	GM/T 0078《密码随机数生成模块设计指南》中，轻量级后处理算法包括下列方法中的（ ）。	冯诺依曼校正器方法	异或链方法	奇偶分组方法	m-LSB方法
2959	多项选择题	GM/T 0078《密码随机数生成模块设计指南》中，基于异或链的后处理方法，下列说法正确的是（ ）。	异或链方法通过将物理随机源输出序列经过多级触发器组合得到内部输出序列	该方法需要异或链的级数与物理随机源序列偏差大小正相关	异或链级数越多，产生随机数效率越低	在实际应用中，至少8级以上的异或链才能清除随机源序列的偏差
2960	判断题	若用一个理想的比较器来量化噪声，将白噪声输出与平均值作比较，则获得的二进制输出序列将会完美地随机。	正确	错误		
2961	判断题	GM/T 0078《密码随机数生成模块设计指南》中，随机数生成模块输出的随机数，依据GM/T 0005进行随机性检测。	正确	错误		

2962	判断题	GM/T 0078《密码随机数生成模块设计指南》中，后处理算法基本原则是不能降低每比特的平均熵，即后处理模块输入n比特，输出m比特，必须保证n≥m，其中n=m的前提是物理随机源输出序列通过GM/T 0005检测。	正确	错误		
2963	判断题	GM/T 0078《密码随机数生成模块设计指南》中，冯诺依曼校正器适用于1出现概率固定,且输出的随机数序列是不相关的随机数生成模块。	正确	错误		
2964	判断题	GM/T 0078《密码随机数生成模块设计指南》中，异或链后处理中，异或链级数越多，则产生随机数的效率越高。	正确	错误		
2965	判断题	GM/T 0078《密码随机数生成模块设计指南》中，基于混沌原理实现物理随机源，需要考虑电路元器件受工艺偏差和寄生效应对的影响，确保电路的稳定工作。	正确	错误		
2966	多项选择题	在GM/T 0013《可信计算 可信密码模块接口符合性测试》中，非对称密钥包含（ ）。	签名密钥	封装密钥	迁移密钥	SM4加解密密钥
2967	多项选择题	在GM/T 0013《可信计算，可信密码模块接口符合性测试》中，为实现规范符合性测试，TCM应具备的能力是（ ）。	能够提供静态度量	能够创建静态测试向量	能够执行动态测试脚本	能够载入和执行来自至少一个其他TCM厂商的TCM数据
2968	多项选择题	在GM/T 0013《可信计算，可信密码模块接口符合性测试》中，测试向量的目的包括（ ）。	确保命令参数的格式正确	确保命令执行结果正确	确保命令参数结构解释正确	确保操作的执行与规范一致
2969	判断题	在GM/T 0013《可信计算，可信密码模块接口符合性测试》中，对厂商而言，TCM符合性测试属于白盒测试。	正确	错误		

2970	判断题	在GM/T 0013《可信计算，可信密码模块接口符合性测试》中，测试向量必须由厂商静态创建。	正确	错误		
2971	判断题	在GM/T 0013《可信计算，可信密码模块接口符合性测试》中，明确命令依赖关系是测试向量和测试脚本正确执行的根本保证。	正确	错误		
2972	判断题	在GM/T 0013《可信计算，可信密码模块接口符合性测试》中，授权协议命令集合依赖于某个实体的授权。	正确	错误		
2973	多项选择题	在GM/T 0013《可信计算可信密码模块符合性检测规范》中，基于TCM厂商和评估者的不同能力，本标准建议采取联合（ ）的方式对TCM进行测试	测试常量	变量	压力测试	集成测试
2974	单项选择题	在GM/T 0013《可信计算可信密码模块符合性检测规范》中，对厂商而言，TCM符合性测试属于（ ）测试，可以直接对这些命令的执行的中间过程进行测试并展示其测试结果	黑盒	白盒	单元	集成
2975	单项选择题	在GM/T 0013《可信计算可信密码模块符合性检测规范》是以（ ）为基础，定义了可信密码模块的命令测试向量，并提供有效的测试方法与灵活的测试脚本	GM/T 0010《SM2密码算法加密签名消息语法规范》	GM/T 0011《可信计算 可信密码支撑平台功能与接口规范》	GM/T 0012《可信计算 可信密码模块接口规范》	GM/T 0058《可信计算 TCM服务模块接口规范》
2976	单项选择题	在GM/T 0079《可信计算平台直接匿名证明规范》中的基于椭圆曲线的直接匿名证明系统中，下列中不属于验证方平台功能的是（ ）。	验证证明数据	认证证明方平台TCM身份	执行TCM_ECDAA_Join命令	请求验证TCM数字身份是否被撤销
2977	单项选择题	在GM/T 0079《可信计算平台直接匿名证明规范》中的基于椭圆曲线的直接匿名证明系统ECDAA中，不属于凭证颁发方的功能的是（ ）。	TCM匿名凭证的申请	初始化ECDAA系统参数	为TCM安全芯片颁发ECDAA凭证	验证TCM安全芯片身份是否撤销

2978	多项选择题	在GM/T 0079《可信计算平台直接匿名证明规范》中，基于椭圆曲线的直接匿名证明系统要求的安全目标包括（ ）。	不可伪造性	机密性	匿名性	不可关联性
2979	判断题	在GM/T 0079《可信计算平台直接匿名证明规范》中的基于椭圆曲线的直接匿名证明系统主要由凭证颁发方、证明方和验证方构成。	正确	错误		
2980	判断题	在GM/T 0079《可信计算平台直接匿名证明规范》中的基于椭圆曲线的直接匿名证明系统的基本流程为系统初始化、凭证颁发、证明和验证。	正确	错误		
2981	判断题	在GM/T 0079《可信计算平台直接匿名证明规范》中，TCM芯片匿名证明实现上可选择支持多个并行匿名证明会话或仅支持单个匿名证明会话。	正确	错误		
2982	判断题	在GM/T 0079《可信计算平台直接匿名证明规范》中的基于椭圆曲线的直接匿名证明系统ECDAA中，证明方根据ECDAA计算位置不同分为主机和TCM安全芯片。	正确	错误		
2983	判断题	在GM/T 0079《可信计算平台直接匿名证明规范》中的基于椭圆曲线的直接匿名证明系统ECDAA中，TCM安全芯片的匿名身份私钥f只允许保存在TCM安全芯片内部。	正确	错误		
2984	单项选择题	在GM/T 0012《可信计算可信密码模块接口规范》中,以下（ ）不是该规范中支持的算法。	SM2	SM3	SM4	SM9
2985	单项选择题	在GM/T 0012《可信计算可信密码模块接口规范》中,可信密码模块是（ ）的集合。	软件	硬件	硬件和固件	固件
2986	单项选择题	在GM/T 0012《可信计算可信密码模块接口规范》中,以下（ ）不是可信密码模块内部的引擎。	对称算法引擎	非对称算法引擎	杂凑算法引擎	管理引擎

2987	单项选择题	在GM/T 0012《可信计算 可信密码模块接口规范》中,以下（ ）为该标准定义和使用的椭圆曲线。	TCM2_ECC_SM2_P256	TCM2_ECC_BN_P256	TCM2_ECC_NIST_P256	TCM2_ECC_NIST_P384
2988	多项选择题	在GM/T 0012《可信计算 可信密码模块接口规范》中,以下（ ）是可信密码模块内部的引擎。	对称算法引擎	非对称算法引擎	杂凑算法引擎	HMAC引擎
2989	多项选择题	在GM/T 0012《可信计算 可信密码模块接口规范》中,非对称算法引擎的是（ ）的单元。	产生非对称密钥	执行非对称加/解密	执行签名运算	执行验签运算
2990	判断题	在GM/T 0012《可信计算 可信密码模块接口规范》中,平台配置寄存器PCR中的数据在芯片复位或者掉电之后数据不会丢失。	正确	错误		
2991	判断题	在GM/T 0012《可信计算 可信密码模块接口规范》中,NV（非易失性存储器）中数据在芯片复位或者掉电之后数据不会丢失。	正确	错误		
2992	判断题	在GM/T 0012《可信计算 可信密码模块接口规范》中,对称算法引擎是执行对称密码运算的单元。	正确	错误		
2993	判断题	在GM/T 0012《可信计算 可信密码模块接口规范》中,TCM2_Startup可以允许成功多次。	正确	错误		
2994	判断题	在GM/T 0012《可信计算 可信密码模块接口规范》中,上电之后，需要先调用TCM2_Startup之后,才能使用其他的功能接口。	正确	错误		
2995	多项选择题	GM/T 0012《可信计算 可信密码模块接口规范》支持（ ）接口。	SM4加密	SM4解密	SM2签名	SM2解密
2996	判断题	在GM/T 0012《可信计算 可信密码模块接口规范》中,平台配置寄存器是可信密码模块内部用于存储平台完整性度量值的存储单元。	正确	错误		
2997	单项选择题	在GM/T 0082《可信密码模块保护轮廓》中，评估对象TOE面临的威胁不包括（ ）。	物理破解	导入	功能异常	密钥溢出

2998	单项选择题	在GM/T 0082《可信密码模块保护轮廓》中，评估对象TOE的安全目的不包括（）。	安全密钥管理	安全销毁	身份标识	完整性检查
2999	单项选择题	在GM/T 0082《可信密码模块保护轮廓》中，强制性原发证明依赖于（）。	选择性原发证明	标识定时	安全属性	无
3000	单项选择题	在GM/T 0082《可信密码模块保护轮廓》中，下列不属于FPT_TST.1（评估对象安全功能TSF检测）中TSF自检程序描述的是（）。	在初始化启动期间运行	正常工作时周期性运行	在授权用户要求时运行	在关闭前运行
3001	单项选择题	在GM/T 0082《可信密码模块保护轮廓》中，ACM_SCP.1（TOE CM范围）要求中，下列不属于CM文档应说明的CM系统应能跟踪的内容是（）。	TOE实现表示	设计文档	维护记录文档	管理员文档
3002	单项选择题	在GM/T 0082《可信密码模块保护轮廓》中，ADV_FSP.1（非形式化功能规范）中不包含（）。	验证者行为元素	开发者行为元素	评估者行为元素	证据的内容和形式元素
3003	多项选择题	在GM/T 0082《可信密码模块保护轮廓》中，评估对象TOE面临的威胁包括（）。	攻击	旁路	冒名	无安全属性
3004	多项选择题	在GM/T 0082《可信密码模块保护轮廓》中，FCS类包含的安全要求有（）。	密钥产生	密钥销毁	密码运算	密钥运算
3005	多项选择题	在GM/T 0082《可信密码模块保护轮廓》中，FPT_FLS.1（带保存安全状态的失败）要求TOE安全功能TSF在（）的情况下应保存一个安全状态	任何密码运算的失败	任何命令或内部操作的失败	密钥泄露	TCM被物理破坏
3006	多项选择题	在GM/T 0082《可信密码模块保护轮廓》中，安全威胁冒名的目的包括（）。	身份标识	安全角色	受保护的功能	安全导入

3007	判断题	在GM/T 0082《可信密码模块保护轮廓》中，评估对象TOE面临的导出威胁是指一个用户或攻击者可能会将数据导出而不附带安全属性或附带的安全属性不够安全，导致导出的数据是错误的并且无效。	正确	错误		
3008	判断题	在GM/T 0082《可信密码模块保护轮廓》中，安全目的的基本原理是通过安全目的与威胁之间的关系证明安全目标的合理性和完整性。	正确	错误		
3009	单项选择题	GM/T 0111《区块链密码应用技术要求》重点对（）类型链的密码安全要素做出规定。	公有链	联盟链	私有链	行业链
3010	单项选择题	GM/T 0111《区块链密码应用技术要求》中规定，在调用智能合约之前，应首先通过密码算法检查链上代码的（）。	真实性	机密性	完整性	抗抵赖性
3011	单项选择题	GM/T 0111《区块链密码应用技术要求》中介绍的区块链的技术架构不包括（）。	数据层	链路层	网络层	应用层
3012	单项选择题	根据GM/T 0111《区块链密码应用技术要求》，在区块链账本中，通常通过区块头的（）识别区块，用于链接相邻区块。	签名值	权限值	杂凑值	时间戳
3013	单项选择题	GM/T 0111《区块链密码应用技术要求》中规定账本存储安全管理满足的要求不包括（）。	区块体不需要进行签名	通过区块头的杂凑值标识区块	采用加密措施保证帐本重要内容机密性	采用身份鉴别和访问控制措施保证账本数据的授权访问
3014	多项选择题	根据GM/T 0111《区块链密码应用技术要求》，区块链是一种物联网、供应链管理、数字资产交易领域的创新应用模式，主要用到了以下选项中的（）技术。	点对点传输	分布式数据存储	密码算法	共识机制
3015	多项选择题	根据GM/T 0111《区块链密码应用技术要求》，在区块链共识层中常见的共识协议包括（）。	PoW	PoS	DPoS	P2P

3016	多项选择题	GM/T 0111《区块链密码应用技术要求》中规定区块链中的数字证书包括（）。	密码设备证书	最终用户数字证书	区块链节点数字证书	OV证书
3017	多项选择题	GM/T 0111《区块链密码应用技术要求》中规定为了满足交易监管要求，通常需要做到（）环节。	用户匿名身份与实体身份的映射关系授权可查看	交易金额或交易信息授权可解密	交易金额授权可修改	交易授权可撤销
3018	判断题	GM/T 0111《区块链密码应用技术要求》中规定区块链的用户注册业务阶段，应生成SM2公私钥，并生成可标识用户的交易地址。	正确	错误		
3019	判断题	根据GM/T 0111《区块链密码应用技术要求》，区块链中用户之间的交易数据，通常以集中账本的形式存储在节点中。	正确	错误		
3020	判断题	根据GM/T 0111《区块链密码应用技术要求》，为提升区块链的时效性，联盟链中支持链外交易模式。	正确	错误		
3021	判断题	根据GM/T 0111《区块链密码应用技术要求》，联盟链中，节点的准入或退出宜采用数字证书技术验证节点身份，并生成审计日志。	正确	错误		
3022	判断题	GM/T 0111《区块链密码应用技术要求》中规定区块链的技术架构从上到下分为应用层、智能合约层、激励层、共识层、网络层和数据层。	正确	错误		
3023	判断题	根据GM/T 0111《区块链密码应用技术要求》，区块链交易中实体鉴别是用户、设备或系统等在区块链网络中交易时，确认实体的身份是否真实。	正确	错误		
3024	单项选择题	GM/T 0122《区块链密码检测规范》中，区块链在账户创建阶段，应生成可以标识用户的（）。	注册地址	交易地址	身份密码	账本密码

3025	单项选择题	GM/T 0122《区块链密码检测规范》中，区块链交易创建时若在区块中包含第三方（），则应符合GM/T 0033《时间戳接口规范》	可信VPN	可信时间戳	可信密码机	可信节点
3026	单项选择题	GM/T 0122《区块链密码检测规范》中，区块链交易创建后需要（）给区块链网络中的节点，然后由节点对交易进行验证，并打包成区块，运行共识协议，保证网路中的节点对所有合法交易达成共识。	广播	多播	单播	以上都是
3027	单项选择题	GM/T 0122《区块链密码检测规范》中，（）是存储在分布式账本中的计算机程序，由区块链用户部署，其任何执行结果都记录在分布式账本中。	共识机制	共识协议	智能合约	交易记录
3028	单项选择题	根据GM/T 0122《区块链密码检测规范》，区块链在部署智能合约时，应检查用户是否获得相应的权限，同时应采用密码技术来保证智能合约（）。	防篡改	防泄漏	防窃取	防病毒
3029	单项选择题	根据GM/T 0122《区块链密码检测规范》，区块链交易创建时应验证有效交易是否能被打包进区块中，通过（）在节点间达成共识。	信任机制	共识机制	互信机制	识别机制
3030	单项选择题	根据GM/T 0122《区块链密码检测规范》，区块链中创建的交易应具有（），应添加nonce值计数等防重放攻击的措施。	独特性	有效性	客观性	唯一性
3031	单项选择题	根据GM/T 0122《区块链密码检测规范》，区块链中链下交易宜采用（）来确认交易各方的真实身份，保存所有交易的审计记录，并采用密码技术保证审计记录的完整性、链外数据的完整性。	对称算法	数字签名	杂凑算法	共识算法
3032	单项选择题	根据GM/T 0122《区块链密码检测规范》，区块链中的随机数应采用经（）的密码部件或模块生成。	商用密码认证	商用密码体系认证	商用密码服务认证	商用密码产品认证

3033	单项选择题	根据GM/T 0122《区块链密码检测规范》，区块链账本存储时应通过（ ）的杂凑值标识区块，用于链接相邻区块，保障区块数据的完整性。	区块	账本	区块头	账本头
3034	单项选择题	根据GM/T 0122《区块链密码检测规范》，区块链密码模块对交易达成共识过程中区块的有效性验证应确保区块中记录的（ ）杂凑值的有效性。	上一个区块	下一个区块	当前区块	以上都是
3035	多项选择题	根据GM/T 0122《区块链密码检测规范》，区块链技术架构可分为数据层、网络层、（ ）和应用层。	传输层	共识层	激励层	智能合约层
3036	多项选择题	根据GM/T 0122《区块链密码检测规范》，区块链中的交易记录包含（ ）等信息。	交易发起者	交易内容	交易接收者	交易发起者的用户签名
3037	多项选择题	根据GM/T 0122《区块链密码检测规范》，区块链密码模块是以区块链技术为核心，用于（ ）、对等网络安全、计算和存储安全、隐私保护、身份认证和管理等的软硬件密码模块。	用户安全	共识安全	物理隔离	账本保护
3038	多项选择题	根据GM/T 0122《区块链密码检测规范》，区块链交易验证时应验证交易记录中的数字签名，确保交易发起者身份的（ ）和交易记录的（ ）。	机密性	真实性	完整性	可用性
3039	多项选择题	根据GM/T 0122《区块链密码检测规范》，区块链通信可在（ ）配置安全通道，以保证数据通信的安全。	各个节点之间	各个区块之间	应用端与区块之间	应用端与节点之间
3040	多项选择题	根据GM/T 0122《区块链密码检测规范》，区块链相关密钥应采取（ ）或（ ）等安全方式进行导入导出。	加密	签名	杂凑	知识拆分
3041	多项选择题	根据GM/T 0122《区块链密码检测规范》，应确保（ ）在区块链密码模块间的可识别性与合法性。	部分节点	所有节点	用户身份	交易信息

3042	多项选择题	根据GM/T 0122《区块链密码检测规范》，区块链中节点和用户身份的鉴别机制应符合（ ）中的一种要求。	GB/T 15843.2《信息技术 安全技术 实体鉴别 第2部分：采用对称加密算法的机制》	GB/T 15843.3《信息技术 安全技术 实体鉴别 第3部分：采用数字签名技术的机制》	GB/T 15843.4《信息技术 安全技术 实体鉴别 第4部分: 采用密码校验函数的机制》	GB/T 15843.5《信息技术 安全技术 实体鉴别 第5部分：使用零知识技术的机制》
3043	判断题	根据GM/T 0122《区块链密码检测规范》，区块链若涉及到密钥分发过程，应具备身份鉴别等保证密钥真实性的安全措施。	正确	错误		
3044	判断题	根据GM/T 0122《区块链密码检测规范》，区块链相关密钥应采取加密或知识拆分等安全方式进行导入导出。	正确	错误		
3045	判断题	根据GM/T 0122《区块链密码检测规范》，区块链中区块的有效性验证应确保区块中记录的下一个区块杂凑值的有效性。	正确	错误		
3046	判断题	根据GM/T 0122《区块链密码检测规范》，区块链在链下交易系统执行周期性的上链操作时，区块链密码模块应检查所有已登记交易的有效性，并根据预先定义的业务规则检查交易清算的正确性。	正确	错误		
3047	判断题	根据GM/T 0122《区块链密码检测规范》，区块链对节点之间的通信数据加密的密钥应有明确的更换周期。	正确	错误		
3048	判断题	根据GM/T 0122《区块链密码检测规范》，区块链中在需要进行实名交易时，应使用数字签名技术鉴别用户身份的合法性及有效性。	正确	错误		
3049	判断题	根据GM/T 0122《区块链密码检测规范》，在区块链中，应确保部分节点和用户身份在区块链密码模块间的可识别性与合法性。	正确	错误		

3050	判断题	根据GM/T 0122《区块链密码检测规范》，区块链中交易创建后需要广播给区块链网络中的节点，然后由节点对交易进行验证。	正确	错误		
3051	判断题	根据GM/T 0122《区块链密码检测规范》，区块链账本存储时应通过区块头的签名值标识区块，用于链接相邻区块，保障区块数据的完整性。	正确	错误		
3052	单项选择题	GM/T 0087《浏览器密码应用接口规范》中的密码接口不包含（）。	加密方法	解密方法	随机数生成方法	派生密钥方法
3053	单项选择题	GM/T 0087《浏览器密码应用接口规范》定义的方法不能完成浏览器中的（）密码功能	用户的认证	文档的签名	文档的加密	通信SSL信道的建立
3054	单项选择题	GM/T 0087《浏览器密码应用接口规范》定义了浏览器执行网页中的密码操作的（）API。	插件	扩展	JavaScript	渲染引擎
3055	多项选择题	GM/T 0087《浏览器密码应用接口规范》中SM4算法不包括（）应用接口。	加密	解密	签名	验签
3056	多项选择题	GM/T 0087《浏览器密码应用接口规范》SM4算法的密钥接口有（）。	生成密钥	导入密钥	导出密钥	派生密钥
3057	多项选择题	GM/T 0087《浏览器密码应用接口规范》SM2签名算法的密钥接口有（）。	生成密钥	导入密钥	导出密钥	派生密钥
3058	判断题	GM/T 0087《浏览器密码应用接口规范》定义了浏览器执行网页中的密码操作的JavaScript API，包括加密、解密、杂凑、签名、签名验证和随机数生成等操作。	正确	错误		
3059	判断题	GM/T 0087《浏览器密码应用接口规范》中的密码接口提供了通用密码功能的接口，其中不包含使用真随机值作为种子的密码学强伪随机数生成器。	正确	错误		

3060	判断题	GM/T 0087《浏览器密码应用接口规范》用于为网络应用中浏览器JavaScript脚本提供密码操作能力。	正确	错误		
3061	单项选择题	GB/T 38636《信息安全技术 传输层密码协议（TLCP）》中规定了握手协议族，不包含在握手协议族内的协议是（）。	密码规格变更协议	报警协议	握手协议	认证协议
3062	单项选择题	GB/T 38636《信息安全技术 传输层密码协议（TLCP）》中规定了主密钥长度为（）个字节。	16	32	48	64
3063	单项选择题	GB/T 38636《信息安全技术 传输层密码协议（TLCP）》中规定在校验算法数据处理时，计算校验码使用的算法是（）。	非对称密码算法	分组密码算法	密码杂凑算法	序列加密算法
3064	单项选择题	GB/T 38636《信息安全技术 传输层密码协议（TLCP）》中规定记录层接收从高层来的任意大小的非空连续数据，在进行压缩后的数据长度最多只能增加（）个字节。	512	1024	2048	4096
3065	单项选择题	GB/T 38636《信息安全技术 传输层密码协议（TLCP）》中规定记录层接收从高层来的任意大小的非空连续数据，将数据分段、压缩、（）、加密，然后传输。	签名	计算校验码	验签	解密
3066	单项选择题	GB/T 38636《信息安全技术 传输层密码协议（TLCP）》中服务端如果找不到与客户端匹配的密码套件，服务端将回应（）报警消息。	serverhello error	serverhello failure	handshake error	handshake failure
3067	单项选择题	GB/T 38636《信息安全技术 传输层密码协议（TLCP）》中规定Certificate Verify消息用于鉴别客户端是否为证书的（）。	颁发者	合法持有者	保管者	信任者
3068	单项选择题	GB/T 38636《信息安全技术 传输层密码协议（TLCP）》中规定，除非出现致命报警，（）在结束连接之前发送关闭通知消息。	客户端	服务端	任何一方都不需要	客户端和服务端任何一方

3069	多项选择题	GB/T 38636《信息安全技术 传输层密码协议（TLCP）》中规定，TLCP协议用到的密码算法包含（ ）。	非对称密码算法	分组密码算法	数据扩展函数和伪随机函数	密码杂凑算法
3070	多项选择题	GB/T 38636《信息安全技术 传输层密码协议（TLCP）》中规定，TLCP协议用到的密钥种类包含（ ）。	服务端密钥	客户端密钥	预主密钥和主密钥	工作密钥
3071	多项选择题	GB/T 38636《信息安全技术 传输层密码协议（TLCP）》中规定，非对称密码算法的用途有（ ）。	身份鉴别	数字签名	密钥交换	报文加密
3072	多项选择题	GB/T 38636《信息安全技术 传输层密码协议（TLCP）》中规定，分组密码算法用于密钥交换数据的加密保护和报文数据的加密保护。可采用的工作模式为（ ）。	GCM	OFB	ECB	CBC
3073	多项选择题	GB/T 38636《信息安全技术 传输层密码协议（TLCP）》中规定，密码杂凑算法的用途为（ ）。	对称密钥生成	机密性	完整性校验	计算安全参数
3074	多项选择题	GB/T 38636《信息安全技术 传输层密码协议（TLCP）》中规定，服务端密钥为非对称密码算法的密钥对，包括的密钥类型有（ ）。	签名密钥对	加密密钥对	HMAC密钥	身份密钥
3075	多项选择题	GB/T 38636《信息安全技术 传输层密码协议（TLCP）》中规定，主密钥（master_secret）由（ ）参数组成，并计算生成的48字节密钥素材，用于生成工作密钥。	预主密钥	客户端随机数	服务端随机数	常量字符串
3076	多项选择题	GB/T 38636《信息安全技术 传输层密码协议（TLCP）》中规定，TLCP包括记录层协议和握手协议族，记录层协议族包括（ ）类型。	密码规格变更协议	报警协议	握手协议	通信协议
3077	多项选择题	GB/T 38636《信息安全技术 传输层密码协议（TLCP）》中规定，记录层协议接收将要被传输的消息，将数据进行（ ）处理。	分块	计算HMAC	加密	传输

3078	多项选择题	GB/T 38636《信息安全技术 传输层密码协议（TLCP）》中规定，连接状态是记录层协议的操作环境。典型的连接状态有（ ）。	当前读状态	当前写状态	未决的读状态	未决的写状态
3079	判断题	GB/T 38636《信息安全技术 传输层密码协议（TLCP）》中规定，如果客户端和服务端决定重用之前的会话，也是需要重新协商安全参数。	正确	错误		
3080	判断题	GB/T 38636《信息安全技术 传输层密码协议（TLCP）》标准只适用于传输层密码协议相关服务器产品，如SSL VPN网关，不适用客户端类产品，如浏览器等的研制。	正确	错误		
3081	判断题	GB/T 38636《信息安全技术 传输层密码协议（TLCP）》中规定，TLCP包括记录层协议和握手协议族，握手协议族包含密码规格变更协议、报警协议及握手协议。	正确	错误		
3082	判断题	GB/T 38636《信息安全技术 传输层密码协议（TLCP）》中规定，报警消息的长度为两个字节，分别为报警级别和报警内容。	正确	错误		
3083	判断题	GB/T 38636《信息安全技术 传输层密码协议（TLCP）》中规定，握手协议不支持IBC的密码算法协商套件。	正确	错误		
3084	判断题	GB/T 38636《信息安全技术 传输层密码协议（TLCP）》中规定，预主密钥（pre_master_secret）是双方协商生成的密钥素材，用于生成主密钥。	正确	错误		

3085	判断题	GB/T 38636《信息安全技术 传输层密码协议（TLCP）》中规定，记录层接收从高层来的任意大小的非空连续数据，将数据分段、压缩、计算校验码、加密，然后传输。接收到的数据经过解密、验证、解压缩、重新封装然后传送给高层应用。	正确	错误		
3086	判断题	GB/T 38636《信息安全技术 传输层密码协议（TLCP）》中规定，握手协议是在记录层协议之下的协议，用于协商安全参数。握手协议的消息通过记录层协议传输。	正确	错误		
3087	单项选择题	在GM/T 0118《浏览器数字证书应用接口规范》中，通过如下（）接口规范调用智能密码钥匙。	CSP	PKCS#11	GM/T 0016《智能密码钥匙密码应用接口规范》（SKF）	GM/T 0020《证书应用综合服务接口规范》（SOF）
3088	单项选择题	在GM/T 0118《浏览器数字证书应用接口规范》中，关于访问证书存储区的权限，下面的描述正确的是（）。	需要对浏览器进行认证授权	需要对USBKey进行认证授权	需要操作系统级别的认证	不需要任何权限
3089	单项选择题	在GM/T 0118《浏览器数字证书应用接口规范》中，关于证书关联智能密码钥匙的方式，下面的描述正确的是（）。	智能密码钥匙的PID/VID	智能密码钥匙中的相关信息，如设备名称、应用名、容器名等	由各个智能密码钥匙厂商自定义实现	由各个浏览器厂商自定义实现
3090	单项选择题	依照GM/T 0118《浏览器数字证书应用接口规范》的定义，在证书存储区中删除证书时，下面的描述正确的是（）。	需要对浏览器进行认证授权后，才能在证书存储区删除证书	需要对USBKey进行认证授权后，才能在证书存储区删除证书	证书一旦写入，不允许删除	不需要任何权限

3091	单项选择题	依照GM/T 0118《浏览器数字证书应用接口规范》的定义，在调用SSF_AddCert将用户证书添加到证书存储区的SSF_CERT_USER_STORE区（证书存储区为用户存储区）时，如果该证书已经被吊销，则下列哪个说法正确的是（）。	SSF_AddCert应报错，不能添加已被吊销的用户证书	SSF_AddCert执行成功	SSF_AddCert弹出警告框，在手动确认后，仍然能被吊销的用户证书添加到证书存储区	各个接口实现厂商自定义该行为
3092	单项选择题	在GM/T 0118《浏览器数字证书应用接口规范》中，对于支持的终端硬件的产品形态，以下描述更准确的是（）。	USBKey	IC卡	TF型智能密码钥匙	不关心具体的产品形态，只要终端安全硬件的调用接口符合GM/T 0016-2012《智能密码钥匙密码应用接口规范》即可
3093	单项选择题	根据GM/T 0118《浏览器数字证书应用接口规范》，对于CRL，如果同一个第三方CA颁发了多个CRL，那么，在证书存储区里，下列描述正确的的是（）。	只能存储第三发CA颁发的最新的CRL	不管CRL的颁发日期，只管按调用SSF_AddCRL的顺序，后添加的CRL覆盖已有的CRL	可存储多个CRL，具体使用哪一个由上层应用决定	对同一个第三方CA，不允许存储多个CRL，在调用SSF_AddCRL报错
3094	多项选择题	在GM/T 0118《浏览器数字证书应用接口规范》定义的证书存储区中，可以存储以下选项中的（）。	用户证书	根证书	CA中间证书	CRL
3095	多项选择题	在GM/T 0118《浏览器数字证书应用接口规范》中，关于证书存储区的描述，下列说法正确的是（）。	定义了证书的存储、枚举、查找、删除等功能	根证书一旦写入，不能删除	定义了CRL的存储、枚举、查找、删除等功能	支持存储RSA证书
3096	多项选择题	在GM/T 0118《浏览器数字证书应用接口规范》中，检查证书状态的方式有（）。	LDAP	CRL	OCSP	未定义获取证书状态的接口

3097	多项选择题	在GM/T 0118《浏览器数字证书应用接口规范》中，关于智能密码钥匙的SKF库（GM/T 0016-2012《智能密码钥匙密码应用接口规范》定义的接口库）管理，下列说法正确的是（ ）。	对于浏览器，只有在智能密码钥匙插入终端设备时，才能将该智能密码钥匙对应的SKF库注册到该浏览器定义的系统环境中	对于浏览器，任何时候都可以将任意一个SKF库注册到该浏览器定义的系统环境中	对于浏览器，最多只能有一个SKF库被注册到该浏览器定义的系统环境中	对于浏览器，可以有任意多个SKF库被注册到该浏览器定义的系统环境中
3098	多项选择题	依照GM/T 0118《浏览器数字证书应用接口规范》的定义，在证书存储区中查找证书时，支持的方式有（ ）。	按证书序列号查找证书	按用户自定义数据查找证书	可按证书算法类型查找RSA算法证书	可按证书存储区类型、证书用途、颁发者等标志组合查找
3099	判断题	在GM/T 0118《浏览器数字证书应用接口规范》中，定义了浏览器使用SM2证书进行加解密、签名验签的接口。	正确	错误		
3100	判断题	浏览器以外的其他应用也可以调用GM/T 0118《浏览器数字证书应用接口规范》定义的接口规范。	正确	错误		
3101	判断题	在GM/T 0118《浏览器数字证书应用接口规范》中，在将用户证书添加到证书存储区时，将自动校验用户证书的有效性，如用户证书的有效性未通过验证，则直接报错，禁止将用户证书添加到证书存储区。	正确	错误		
3102	单项选择题	根据GM/T 0039《密码模块安全检测要求》，关于密码模块逻辑接口描述不正确的是（ ）。	密码模块逻辑接口应当是相互分离的	输入数据和输出数据可以共享同一个物理端口	逻辑接口可以分布在一个或多个物理端口上	输入数据和输出数据不可以使用同一个物理端口
3103	单项选择题	根据GM/T 0039《密码模块安全检测要求》，送检单位的密码模块应包括（ ）密码主管角色。	一个	两个	至少一个	至少两个

3104	判断题	根据GM/T 0039《密码模块安全检测要求》，如果密码模块支持基于角色的鉴别机制，那么模块应当要求操作员隐式或显式地选择一个或多个角色。	正确	错误		
3105	单项选择题	根据GM/T 0039《密码模块安全检测要求》，每一个密码模块的实例应当能够（ ）自己的SSP。	分享和修改	分享和支配	控制和修改	控制和支配
3106	单项选择题	根据GM/T 0039《密码模块安全检测要求》，针对多芯片嵌入式密码模块，以下属于安全二、三级密码模块要求的是（ ）。	拆卸响应	置零电路	拆卸存迹	拆卸检测封套
3107	单项选择题	根据GM/T 0039《密码模块安全检测要求》，如果熵是从模块密码边界外部收集的，那么使用该熵作为输入所生成的数据流应当被视为（ ）。	CSP	SSP	PSP	ESP
3108	单项选择题	根据GM/T 0039《密码模块安全检测要求》，以下关于可信信道，说法错误的是（ ）。	可信信道使用的物理端口应当与其他物理端口实现物理隔离	可信信道应当采用SSL协议，用于在密码模块与发送者或接受者终端之间传输数据	可信信道使用的逻辑接口应当与其他逻辑接口实现逻辑隔离	基于身份的鉴别应当用于所有使用可信信道的服务
3109	单项选择题	根据GM/T 0039《密码模块安全检测要求》，以下关于敏感安全参数（SSP），说法正确的是（ ）。	SSP被置零后可以从模块中恢复和重用	密码模块应当对受保护的SSP执行置零	模块应当在SSP置零完成时提供输出状态指示	应当禁止授权操作员修改SSP
3110	多项选择题	根据GM/T 0039《密码模块安全检测要求》，检测机构可以以下面一个或多个方式对密码模块的安全性进行测试（ ）。	检测人员使用检测机构的设备进行测试	检测人员使用送检单位的设备进行测试	送检单位的检测人员使用检测机构的设备进行测试	检测人员监督送检单位使用送检单位的设备进行测试
3111	多项选择题	根据GM/T 0039《密码模块安全检测要求》，密码模块除数据输入、输出接口外，还应当具备下列接口（ ）。	控制输入接口	状态输出接口	状态输入接口	控制输出接口

3112	多项选择题	根据GM/T 0039《密码模块安全检测要求》，密码模块应当采用物理安全机制以限制对模块内容的非授权物理访问，并阻止对已安装模块的非授权使用或修改，检测人员应核实模块（ ）的物理安全保护机制。	硬件	软件	固件	数据
3113	多项选择题	根据GM/T 0039《密码模块安全检测要求》，对于二级及以上的多芯片独立式密码模块，如果其外壳含有任何门或封盖，则下列保护机制中可行的是（ ）。	带有物理或逻辑钥匙的防撬机械锁	存迹胶带	全息封条	防尘网
3114	多项选择题	根据GM/T 0039《密码模块安全检测要求》，所有进出密码模块的逻辑信息流，都应当仅通过已定义的物理端口和逻辑接口。送检文档中应通过（ ）说明密码模块的信息流和物理接入点。	框图	设计规格	源代码	原理图
3115	多项选择题	根据GM/T 0039《密码模块安全检测要求》，关于密码模块的工作模式说法正确的是（ ）。	操作员应当能够在核准的工作模式下操作模块	核准的工作模式应当定义为一组服务的集合，其中至少有一个服务使用了核准的密码算法、安全功能或过程	核准的和非核准的服务和工作模式的CSP应当相互分离	非核准的密码算法或非核准的密钥生成方式可能被用来混淆数据或CSP，但是结果被视为未受保护的明文，且只能提供非安全相关功能
3116	多项选择题	根据GM/T 0039《密码模块安全检测要求》，关于非入侵式安全，以下属于安全三级密码模块要求的是（ ）。	如果有相应措施，文档应当包括可以证明每个缓解技术有效性的证据	密码模块应当实现用于保护CSP免受GM/T 0028附录F中的所有非入侵式攻击的缓解技术	密码模块应当接受测试以满足核准的非入侵式攻击缓解测试指标的要求	文档应当包括可以证明每个环节技术有效性的证据，并提供测试方法

3117	判断题	根据密码模块相关标准，在密码模块中，用户角色应当负责执行密码初始化或管理功能，以及常用的安全服务。	正确	错误		
3118	判断题	根据密码模块相关标准，密码模块鉴别操作员仅可采用对称加密算法或数字签名技术的鉴别机制。	正确	错误		
3119	判断题	根据密码模块相关标准，用于核准的工作模式的非安全相关的算法、安全功能、过程和部件的实现应当不干扰或破坏密码模块核准的工作模式的运行。	正确	错误		
3120	判断题	根据密码模块相关标准，检测人员应核实当密码模块处于错误状态时，应当禁止通过“状态输出”接口输出当前状态。	正确	错误		
3121	判断题	根据密码模块相关标准，置零可以使用一个未受保护的SSP来覆盖另一个未受保护的SSP。	正确	错误		
3122	判断题	根据密码模块相关标准，手动输入条件测试可以采用两种方式之一：错误检测码或两次重复密钥录入。	正确	错误		
3123	判断题	根据密码模块相关标准，对于密码模块的每一个物理或逻辑的输入，以及物理或逻辑的输出，材料中应明确逻辑接口所对应的物理输入或输出。	正确	错误		
3124	判断题	根据密码模块相关标准，如果密码模块支持核准和非核准的工作模式，密码模块的安全策略文档中应为模块所包括的核准的工作模式定义完整的服务集合，不需要为非核准的工作模式定义服务集合。	正确	错误		
3125	判断题	根据密码模块相关标准，当进入或退出维护员角色时，所有SSP应当被置零。	正确	错误		

3126	判断题	根据密码模块相关标准，对于安全一、二级的软件模块或混合软件模块的软件部件，CSP、密钥分量和鉴别数据可以以加密或明文的形式输入或输出运行环境。	正确	错误		
3127	判断题	根据密码模块相关标准，密码模块应当按照各个域的要求进行测试。密码模块的整体安全级别为各个域中评估安全级别的最高等级。	正确	错误		
3128	多项选择题	根据GM/T 0039《密码模块安全检测要求》，关于密码模块物理安全描述正确的是（）。	安全二级增加了拆卸存迹机制的要求，以及确保无法对模块关键区域的内部操作收集信息的要求	安全三级增加了使用坚固或硬质的保形或不保形外壳的要求，要求外壳的封盖和门具有拆卸检测和响应机制，并且要求抵抗通过开口或入口的直接探测	安全四级要求具备环境失效保护（EFP），以防止错误注入攻击	当密码模块被设计成允许物理访问时，需要为维护访问接口规定安全要求。拆卸检测和拆卸响应可以代替显式的拆卸证据
3129	单项选择题	根据GM/T 0039《密码模块安全检测要求》，以下不属于常见的错误注入技术的为（ ）。	电压	辐射	拆除外壳	时钟
3130	单项选择题	根据GM/T 0083《密码模块非入侵式攻击缓解技术指南》，对于信道泄露的高级利用主要依赖于以下的（）。	加密算法的明文信息	加密算法产生的密文信息	加密算法本身	密码设备处理的数据以及检索秘密参数时执行的操作
3131	单项选择题	根据GM/T 0083《密码模块非入侵式攻击缓解技术指南》，关键安全参数不包括下列选项中的（）。	私有密码密钥	口令等鉴别信息	密码算法密文信息	个人身份证号
3132	单项选择题	根据GM/T 0083《密码模块非入侵式攻击缓解技术指南》，在非入侵式攻击缓解技术中，下列不属于计时分析缓解技术的是（）。	平衡指令分支技术	低功耗技术	随机延时插入技术	盲化技术
3133	单项选择题	根据GM/T 0083《密码模块非入侵式攻击缓解技术指南》，在非入侵式攻击缓解技术中，下列不属于时间维度的隐藏技术的是（）。	随机插入伪指令技术	伪轮运算技术	时钟随机化技术	双轨预充电逻辑

3134	单项选择题	根据GM/T 0083《密码模块非入侵式攻击缓解技术指南》，在非入侵式攻击缓解技术中，下列不属于振幅维度的隐藏技术的是（ ）。	低功耗设计技术	复合寄存器技术	平衡指令分支技术	双轨预充电逻辑
3135	单项选择题	根据GM/T 0083《密码模块非入侵式攻击缓解技术指南》，电磁分析攻击缓解技术不包括下列选项中的（ ）。	低功耗技术	平衡指令分支技术	扩展频谱时钟技术	交错的双轨逻辑技术
3136	单项选择题	根据GM/T 0083《密码模块非入侵式攻击缓解技术指南》，下列关于非入侵式攻击测试的说法哪个不正确的是（ ）。	非入侵式攻击测试需要从密码模块中或者周围提取物理量	非入侵式攻击测试主要利用隐藏在物理量中的有偏性展开攻击	非入侵式攻击测试能够保证密码模块可完全抵抗攻击	非入侵式攻击测试限制条件包括测试时间和数据收集的最大上限
3137	单项选择题	下列不属于GM/T 0083《密码模块非入侵式攻击缓解技术指南》中的测试内容的是（ ）。	计时分析攻击	简单能量分析	差分电磁分析	缓存攻击分析
3138	单项选择题	根据GM/T 0083《密码模块非入侵式攻击缓解技术指南》，在非入侵式攻击测试中，下列关于核心测试流程的说法正确的是（ ）。	无需核对指定关键安全参数的厂商文档	只需要测试一个关键安全参数类即可	测试流程中只要有一部分关键安全参数通过了测试则认为通过测试	若一个核心测试由于设定的重复操作次数上限而无法继续进行，则认为通过测试
3139	单项选择题	根据GM/T 0083《密码模块非入侵式攻击缓解技术指南》，下列关于简单能量/电磁泄露测试流程的说法错误的是（ ）。	测试实验室应根据期望达到的安全能力获取对应数量的侧信道测量信息	测试实验室进行密码算法指令序列识别分析	指令序列相关性的识别方法包括交叉关联方法以及聚类分析方法	可以根据测试人员的主观判断来确认指令序列的相关性
3140	单项选择题	根据GM/T 0083《密码模块非入侵式攻击缓解技术指南》，下列关于差分能量/电磁泄露测试流程的说法错误的是（ ）。	测试实验室应根据期望达到的安全能力来获取对应数量的侧信道测量信息	可以使用校准函数进行静态或动态的曲线对齐操作分析方法	检测侧信道中是否存在敏感信息泄露需要使用统计分析方法	测试实验室无需预先指定测试向量集合，可直接使用随机测试向量开始测试
3141	多项选择题	根据GM/T 0083《密码模块非入侵式攻击缓解技术指南》，技术人员应当（ ）选择缓解技术来抵抗非入侵式攻击。	根据具体的密码算法特点	根据密码模块的特性	根据具体部署的实际场景	任选一种缓解技术即可实现完全的保护

3142	多项选择题	根据GM/T 0083《密码模块非入侵式攻击缓解技术指南》，以下选项属于简单侧信道分析的是（）。	差分能量分析	互信息能量分析	简单能量分析	简单电磁分析
3143	多项选择题	根据GM/T 0083《密码模块非入侵式攻击缓解技术指南》，以下选项属于基于统计学的侧信道分析的是（）。	互信息分析	极大似然分析	相关性分析	简单能量分析
3144	多项选择题	根据GM/T 0083《密码模块非入侵式攻击缓解技术指南》，以下选项属于高级侧信道分析的通用步骤的是（）。	对观测量进行多次观测	直接通过肉眼识别的方式对密码模块的能量泄露进行检测	为设备选择泄露模型	对密钥或者子密钥的可能值进行假设
3145	多项选择题	根据GM/T 0083《密码模块非入侵式攻击缓解技术指南》，非入侵式攻击的工作方式包括（）。	水平攻击	垂直攻击	矩形攻击	计时攻击
3146	单项选择题	根据GM/T 0083《密码模块非入侵式攻击缓解技术指南》，简单侧信道分析和高级侧信道分析的区别是（）。	是否使用了统计分析方法	是否采集了侧信道物理量	分析对象是否是分组密码算法	分析对象是否是非对称密码算法
3147	多项选择题	根据GM/T 0083《密码模块非入侵式攻击缓解技术指南》，在非入侵式攻击缓解技术中，时间维度的隐藏技术包括（）。	随机插入伪指令技术	伪轮运算技术	时钟随机化技术	乱序操作技术
3148	多项选择题	根据GM/T 0083《密码模块非入侵式攻击缓解技术指南》，在非入侵式攻击缓解技术中，振幅维度的隐藏技术包括（）。	双轨预充电逻辑	信号滤波与噪声叠加	低功耗技术	复合寄存器技术
3149	多项选择题	根据GM/T 0083《密码模块非入侵式攻击缓解技术指南》，在非入侵式攻击缓解技术中，掩码缓解技术说法正确的是（）。	可对密码算法计算过程中产生的中间值进行随机化处理	可分为1阶，2阶，n阶掩码方案	掩码方案阶数越高开销越小	通常情况下，掩码方案阶数越高安全性越高
3150	多项选择题	根据GM/T 0083《密码模块非入侵式攻击缓解技术指南》，在非入侵式攻击缓解技术中，下列关于混合缓解技术的说法正确的是（）。	采用混合缓解技术可以保证密码算法绝对安全	采用混合缓解技术比单种缓解技术的开销更小	采用混合缓解技术通常是为了兼顾安全性以及资源开销	混合缓解技术相比单一缓解技术为密码算法带来了更高的安全性

3151	判断题	根据GM/T 0083《密码模块非入侵式攻击缓解技术指南》，高级侧信道分析主要依赖于密码设备处理的数据以及检索秘密参数时执行的操作。	正确	错误		
3152	判断题	关键安全参数的泄露或修改不会危及密码模块的安全。	正确	错误		
3153	判断题	根据GM/T 0083《密码模块非入侵式攻击缓解技术指南》，在非入侵式攻击缓解技术中，垂直攻击指的是从单次算法执行过程中提取敏感信息的方法。	正确	错误		
3154	判断题	根据GM/T 0083《密码模块非入侵式攻击缓解技术指南》，在非入侵式攻击缓解技术中，关键安全参数的分类，包括密钥、鉴别数据（如口令、PINs码、生物鉴别数据）等。	正确	错误		
3155	判断题	根据GM/T 0083《密码模块非入侵式攻击缓解技术指南》，在非入侵式攻击缓解技术中，水平攻击指的是从多条能量迹中的相同部分提取敏感信息的方法。	正确	错误		
3156	判断题	根据GM/T 0083《密码模块非入侵式攻击缓解技术指南》，在非入侵式攻击缓解技术中，垂直攻击指的是从单条能量迹中的不相同部分提取敏感信息的方法。	正确	错误		
3157	判断题	根据GM/T 0083《密码模块非入侵式攻击缓解技术指南》，电磁分析是对密码模块中由于逻辑电路转化所造成的电磁辐射的分析。	正确	错误		

3158	判断题	根据GM/T 0083《密码模块非入侵式攻击缓解技术指南》，简单能量分析是对指令执行（或单个指令的执行）模式的直接（主要是可视化的）分析，它与密码模块的能耗有关，并用以获取密码操作相关的信息。	正确	错误		
3159	判断题	根据GM/T 0083《密码模块非入侵式攻击缓解技术指南》，在非入侵式攻击缓解技术中，计时分析是对安全功能中某个操作的响应或执行时间变化进行分析，这种时间变化可能揭露出与诸如密钥或PIN等安全参数有关的信息。	正确	错误		
3160	判断题	根据GM/T 0083《密码模块非入侵式攻击缓解技术指南》，简单电磁分析是通过测量电磁辐射对指令执行模式和逻辑电路活动模式的直接（主要是可视化的）分析。	正确	错误		
3161	单项选择题	GM/T 0084《密码模块物理攻击缓解技术指南》中规定的物理安全因素不包括以下哪个因素（）。	体积	混合和分层的机制	空间和环境	重量
3162	单项选择题	GM/T 0084《密码模块物理攻击缓解技术指南》中通过将VCC变更为异常的高值或低值，在电路中诱发异常行为的攻击指的的哪种攻击（）。	高电压数据印痕攻击	手工材料移除	高低压异常攻击	聚能切割
3163	单项选择题	GM/T 0084《密码模块物理攻击缓解技术指南》中通过RFID轮询技术，能够对哪种攻击进行检测（）。	辐射数据印痕攻击	物理位置改变或替换	高电压数据印痕攻击	时钟毛刺
3164	单项选择题	GM/T 0084《密码模块物理攻击缓解技术指南》中规定的内部探针不包括以下哪种探针（）。	能量探针	震动探针	被动式探针	主动式探针

3165	单项选择题	GM/T 0084《密码模块物理攻击缓解技术指南》中，通过调整运行电压或温度，或扰乱时钟以改变频率，使设备电路超出正常运行范围的上界或下界，迫使设备进入不可预知的状态的攻击指的是哪种攻击（）。	设备电路失效攻击	设备电压失效攻击	设备温度失效攻击	设备时钟失效攻击
3166	多项选择题	GM/T 0084《密码模块物理攻击缓解技术指南》中规定物理安全所涉及的攻击缓解技术包含以下哪种技术（）。	篡改抵抗类技术	篡改响应类技术	篡改检测类技术	篡改存迹类技术
3167	单项选择题	GM/T 0084《密码模块物理攻击缓解技术指南》中规定的篡改检测技术不包含哪种传感器（）。	电压传感器	探针传感器	剂量传感器	动作传感器
3168	单项选择题	GM/T 0084《密码模块物理攻击缓解技术指南》中规定在密码模块发布之前，应被移除、禁用或不提供给攻击者使用的不包括以下哪一项（）。	测试探针接入口	出厂安装密钥	阵列中内置自测试管脚	固件断点
3169	单项选择题	GM/T 0084《密码模块物理攻击缓解技术指南》中规定配送环节中的物理攻击缓解方法不包括以下哪种方法（）。	为用户提供包含设计规格、图表、图纸、插图及物理安全机制信息的文档	提供适当的模块化打包方式以确保密码模块的安全性	采取一些流程以证明配送中密码模块未受到破坏	对用户进行培训以保证密码模块的正确使用
3170	判断题	GM/T 0084《密码模块物理攻击缓解技术指南》中数据印痕攻击指的是通过采取措施（例如辐射、高温等）将内存电路或包含敏感信息的设备中的数据进行固化，使得在一段时间内，不能对数据进行写入、修改等操作。	正确	错误		
3171	判断题	密码模块仅在使用时存在物理安全威胁。	正确	错误		

3172	判断题	GM/T 0084《密码模块物理攻击缓解技术指南》定义的防篡改是指抵抗所有已知攻击和可能的突发攻击的物理安全机制。	正确	错误		
3173	判断题	GM/T 0084《密码模块物理攻击缓解技术指南》中定义的内部探针攻击是指通过探针直接接触电路中导体的方式，获得密码模块信息和/或对密码模块进行修改。	正确	错误		
3174	判断题	GM/T 0084《密码模块物理攻击缓解技术指南》中规定的机械加工是指一种利用机械设备、可在短时间内完成的材料移除方法。	正确	错误		
3175	判断题	GM/T 0084《密码模块物理攻击缓解技术指南》定义的时钟毛刺是指通过对时钟电路注入一个短时间高电压脉冲信号，在电路中诱发异常行为。	正确	错误		
3176	判断题	GM/T 0084《密码模块物理攻击缓解技术指南》中的能量攻击技术定义的激光 / 放射线读 / 写是指通过使用激光 / 放射线直接穿透芯片的硅外壳部分，对计算设备的存储单元进行读写操作。	正确	错误		
3177	判断题	GM/T 0084《密码模块物理攻击缓解技术指南》中的缓解技术是否能够成功抵抗特定的物理攻击，与密码模块的物理特性、特定物理攻击强度、缓解技术参数指标的选取等因素相关。	正确	错误		
3178	判断题	GM/T 0084《密码模块物理攻击缓解技术指南》中定义的抛光包装是属于篡改存迹类的缓解攻击技术。	正确	错误		
3179	判断题	GM/T 0084《密码模块物理攻击缓解技术指南》中微偏移动作传感器是指通过检测微偏移动作传感器变化的方式，对密码模块是否发生形变进行检测。	正确	错误		

3180	多项选择题	GM/T 0084《密码模块物理攻击缓解技术指南》中，下列哪些选项属于能量攻击（）。	喷砂处理	时钟毛刺	电磁干扰	成像方法
3181	多项选择题	GM/T 0084《密码模块物理攻击缓解技术指南》中，以下哪些属于篡改抵抗类技术（）。	坚硬的外壳	绝缘基板	不透明	特殊半导体拓扑
3182	多项选择题	GM/T 0084《密码模块物理攻击缓解技术指南》中，以下哪些属于篡改检测类技术（）。	气体分析	电压传感器	超声波传感器	压电片
3183	多项选择题	GM/T 0084《密码模块物理攻击缓解技术指南》中，以下哪些属于篡改响应类技术（）。	RAM掉电	使用铝热剂	消磁	PUF响应
3184	多项选择题	GM/T 0084《密码模块物理攻击缓解技术指南》规定的在开发过程中可以阻止或缓解物理攻击的方法有（）。	进行安全测试	移除、禁用测试调试机制	预装密钥	提供攻击反馈
3185	多项选择题	GM/T 0084《密码模块物理攻击缓解技术指南》中，以下哪些不属于篡改存迹类技术（）。	压电片	易碎包装	消磁	一次性应力形变测试仪
3186	多项选择题	GM/T 0084《密码模块物理攻击缓解技术指南》中，以下哪些属于加工技术（）。	手工材料移除	聚能切割	水刀加工	喷砂处理
3187	单项选择题	GM/T 0028《密码模块安全技术要求》中规定的密码模块不包括以下哪种类型（）。	硬件模块	软件模块	混合固件模块	混合硬件模块
3188	单项选择题	GM/T 0028《密码模块安全技术要求》中的“核准的安全功能”不包括以下哪项（）。	入侵检测	数字签名	密钥协商	实体鉴别
3189	单项选择题	GM/T 0028《密码模块安全技术要求》中对于（）不提供三级和四级安全要求。因此，在该条件下，软件密码模块最高仅为安全二级。	可修改运行环境	软件/固件安全	物理安全	敏感安全参数管理
3190	单项选择题	根据GM/T 0028《密码模块安全技术要求》的要求，对于安全四级，密码模块应当采用（）以控制对模块的访问。	基于身份的多因素鉴别机制	基于角色的鉴别机制	不要求采用鉴别机制	基于身份的多因素鉴别机制或者基于角色的鉴别机制

3191	单项选择题	根据GM/T 0028《密码模块安全技术要求》的要求，（ ）级及以上密码模块手动建立的敏感安全参数需要以加密的形式、通过可信信道或使用知识拆分过程输入或输出。	1	2	3	4
3192	单项选择题	根据GM/T 0028《密码模块安全技术要求》的要求，（ ）级及以上等级的密码模块要求基于身份的鉴别机制。	1	2	3	4
3193	单项选择题	根据GM/T 0028《密码模块安全技术要求》的要求，（ ）级的密码模块密码边界内的所有软件和固件应当使用核准的数字签名进行保护。	1	2	2和3	3和4
3194	单项选择题	根据GM/T 0028《密码模块安全技术要求》的要求，以下哪个不属于安全三级的“物理安全”通用要求（ ）。	产品级部件	拆卸检测和响应封套	防止通过孔和缝进行探测	针对温度和电压的EFP或EFT
3195	单项选择题	GM/T 0028《密码模块安全技术要求》要求，无论熵从密码边界内部还是外部收集，对任何一个关键安全参数，其最小熵值应当不小于（ ）比特。	128	192	224	256
3196	单项选择题	GM/T 0028《密码模块安全技术要求》规定，运行在通用计算机上的软件密码模块所处的运行环境是（ ）。	可修改的运行环境	受限的运行环境	不可修改的运行环境	不受限的运行环境
3197	单项选择题	根据GM/T 0028《密码模块安全技术要求》，如果密码模块使用了知识拆分过程，模块应当使用（ ）的操作员鉴别，分别鉴别每个密钥分量的输入或输出，而且应至少需要（ ）密钥分量来重建原来的密钥	基于身份，2个	基于角色，2个	基于身份，3个	基于角色，3个
3198	单项选择题	GM/T 0028《密码模块安全技术要求》要求，（ ）不应视为软件密码模块的密码边界内的组件。	密码模块的可执行文件	密码模块的源代码	在内存中的密码模块实例	密码模块的可执行文件集合
3199	单项选择题	根据GM/T 0028《密码模块安全技术要求》，哪项不是密码模块三级要求（ ）。	基于身份的鉴别	多因素鉴别	拆卸响应	EFP或EFT

3200	单项选择题	GM/T 0028《密码模块安全技术要求》中规定的密码模块硬件封装形式不包括以下哪种类型（）。	单芯片	单芯片独立式	多芯片嵌入式	多芯片独立式
3201	单项选择题	以下哪个部件不能作为GM/T 0028《密码模块安全技术要求》中规定的密码模块控制输入接口（）。	LED指示灯	触摸屏	芯片管脚	网口
3202	多项选择题	下列哪些选项是GM/T 0028《密码模块安全技术要求》规定的安全域（）。	角色/服务/鉴别	自测试	有限状态模型	密码算法
3203	多项选择题	根据GM/T 0028《密码模块安全技术要求》，对于运行于可修改环境中的密码模块，以下哪些安全域要求必须适用的（）。	物理安全	运行环境	软件/固件安全	自测试
3204	多项选择题	以下哪项是GM/T 0028《密码模块安全技术要求》所认为的非入侵式攻击（）。	能量分析	计时分析	电磁泄露	穷举攻击
3205	多项选择题	GM/T 0028《密码模块安全技术要求》要求，密码算法条件自测试可以是（）。	已知答案测试	对比测试	错误检测测试	性能测试
3206	多项选择题	哪些是GM/T 0028《密码模块安全技术要求》所认为的敏感安全参数（）。	对称密钥	私钥	公钥	口令
3207	多项选择题	根据GM/T 0028《密码模块安全技术要求》，以下说法正确的是（）。	可以为密码模块的某一个安全域进行单独检测，而不对其他安全域进行检测	密码模块将获得一个整体评级，整体评级设定为 11 个域所获得的最低评级。	一些域的安全要求不分安全等级，那么密码模块在这些域中将获得与整体评级相当的评级。	安全一级密码模块保护的信息资产价值应当是较低的，且外部环境已经具备相对较好的控制措施
3208	多项选择题	根据GM/T 0028《密码模块安全技术要求》，对于软件密码模块，以下哪些要求是可选的（）。	物理安全	运行环境	身份鉴别	非入侵式攻击
3209	多项选择题	根据GM/T 0028《密码模块安全技术要求》，软件密码模块包括以下哪些输入接口（）。	电源输入接口	数据输入接口	控制输入接口	状态输入接口
3210	多项选择题	以下哪些属于GM/T 0028《密码模块安全技术要求》生命周期保障中的安全要求项（）。	有限状态模型	配置管理	厂商测试	指南文档

3211	多项选择题	根据GM/T 0028《密码模块安全技术要求》，以下哪项是密码模块管理员指南应当阐明的内容（）。	密码主管和/或其他管理角色可用的密码模块的管理功能、安全事件、安全参数(以及适当的参数值)、物理端口以及逻辑接口。	密码模块内部利用随机数生成器生成密钥的原理	独立的操作员鉴别机制能够独立起作用所需的流程	与密码模块安全操作相关的用户行为的假定
3212	多项选择题	根据GM/T 0028《密码模块安全技术要求》，以下说法正确的是（）。	只要选择了符合要求的密码模块，那么相关密码应用就是安全的	密码模块相应的安全等级，需要密码模块产品和其安全策略的配合来保证	一般而言，安全等级越高的密码模块，安全策略越简单	安全策略文件说明了密码模块运行应遵从的安全规则，包含了从密码模块安全要求标准导出的规则及厂商要求的规则
3213	多项选择题	根据GM/T 0028《密码模块安全技术要求》的要求，如果密码模块可以从外部加载软件或固件，下列说法正确的是（ ）。	密码模块应当实现核准的鉴别技术以验证加载软件或固件是经过审验的	核准的鉴别技术所需的鉴别密钥可以伴随软件或固件，加载到模块中	软件/固件的有效性应当成功通过核准的鉴别技术的验证，否则软件/固件加载测试应当失败。	如果软件/固件加载测试失败，则不应当使用加载的软件或固件
3214	判断题	根据GM/T 0028《密码模块安全技术要求》，能量分析攻击一般需要通过物理入侵密码模块才能完成。	正确	错误		
3215	判断题	根据GM/T 0028《密码模块安全技术要求》，密码模块必须至少具备“密码主管”和“用户”两种角色。	正确	错误		
3216	判断题	根据GM/T 0028《密码模块安全技术要求》，对于直接输入的敏感安全参数，输入值可以长时间显示出来，以验证输入的正确性。	正确	错误		

3217	判断题	GM/T 0028《密码模块安全技术要求》要求，软件/固件安全域不适用于硬件密码模块。	正确	错误		
3218	判断题	GM/T 0028《密码模块安全技术要求》要求，与软件密码模块类似，固件密码模块的物理安全域也是可选的。	正确	错误		
3219	判断题	根据GM/T 0028《密码模块安全技术要求》，软件密码模块的运行环境所包含的计算平台和操作系统，在定义的密码边界之外。	正确	错误		
3220	判断题	根据GM/T 0028《密码模块安全技术要求》，密码算法条件自测试必须在密码模块上电时全部执行完毕。	正确	错误		
3221	判断题	GM/T 0028《密码模块安全技术要求》中的“生命周期保障”安全域，主要考虑的是对密钥的全生命周期管理。	正确	错误		
3222	判断题	根据GM/T 0028《密码模块安全技术要求》，密码模块不能从外部收集熵用于随机数的产生。	正确	错误		
3223	判断题	GM/T 0028《密码模块安全技术要求》中，关键安全参数是与安全相关的秘密信息，被泄露或被修改后会危及密码模块的安全性。CSP必须是经过加密的。	正确	错误		
3224	判断题	GM/T 0028《密码模块安全技术要求》中，密码主管是由个体或代表个体操作的进程所担任的角色，该角色负责执行密码模块的密码初始化或管理功能。	正确	错误		
3225	判断题	GM/T 0028《密码模块安全技术要求》中，数据路径是数据通过的物理或逻辑通道，多条逻辑数据路径必须使用不同的物理数据路径。	正确	错误		

3226	多项选择题	GM/T 0028《密码模块安全技术要求》中，密码边界是明确定义的连续边线，该边线建立了密码模块的物理和/或逻辑边界，并包括了密码模块的所有（）。	硬件部件	软件部件	固件部件	包装部件
3227	多项选择题	GM/T 0028《密码模块安全技术要求》中，常见的错误注入技术包括通过应用短暂的（ ）技术，导致硬件中的操作行为发生变化的技术。	电压	辐射	激光	时钟偏移
3228	多项选择题	根据GM/T 0028《密码模块安全技术要求》，公开安全参数是与安全性相关的公开信息，一旦被修改，会威胁到密码模块安全。以下为公开安全参数的为（）	公钥	自签名证书	签名私钥	信任锚
3229	多项选择题	根据GM/T 0028《密码模块安全技术要求》，角色是与用户关联的安全属性，它定义了对密码模块服务的访问权限。关于角色的描述正确的是（）。	一个角色可以与一个或多个服务相关联	一个用户只能担任一个角色	一个角色可以与一个或多个用户相关联	一个用户可以担任一个或多个角色
3230	多项选择题	根据GM/T 0028《密码模块安全技术要求》，以下为密码模块安全二级要求的是（）。	拆卸证据机制或者防撬锁机制，以提高物理安全性	基于角色的鉴别机制	软件密码模块可以运行在可修改的环境中	基于身份的鉴别机制
3231	多项选择题	根据GM/T 0028《密码模块安全技术要求》，以下为密码模块安全三级要求的是（）。	置零响应电路	软件密码模块可以运行在可修改的环境中	基于身份的鉴别机制	有效防止电压、温度超出模块正常运行范围对密码模块安全性的破坏

3232	多项选择题	根据GM/T 0028《密码模块安全技术要求》，关于可信信道说法正确的是（）。	对于安全一级和二级，没有可信信道要求	对于安全三级，密码模块应当实现可信信道，用于在密码模块与发送者或接收者终端之间传输未保护的明文CSP、密钥分量以及鉴别数据	可信信道使用的逻辑接口可与其它逻辑接口复用	可信信道使用的物理端口应当与其它物理端口实现物理隔离
3233	多项选择题	GM/T 0028《密码模块安全技术要求》中，旁路能力是指某种服务所具备的部分或全部绕过密码功能的能力。如果密码模块实现了旁路能力，那么（）。	在开启密码模块的旁路功能之前，操作员应当担任相应的授权角色	使用一个内部操作来激活旁路能力，以防止不经意地输出明文数据	模块应当显示其状态以指示旁路能力是否：未被激活	模块应当显示其状态以指示旁路能力是否：被激活
3234	单项选择题	根据GM/T 0028《密码模块安全技术要求》，以下不属于密码模块接口类型的是（）。	数据输入接口	数据输出接口	状态输入接口	控制输出接口
3235	单项选择题	根据GM/T 0028《密码模块安全技术要求》，如果密码模块具有加载外部软件或固件的能力，那么下列要求描述不正确的是（）。	加载的软件或固件应当在加载之前经过审验机构的审验，以维持审验效力	应当维持模块的版本信息	应当禁止通过数据输出接口输出数据，直到软件/固件加载完成以及加载测试成功通过	密码模块应当拒绝运行任何已经加载的或已被修改的核准安全功能，直到成功执行运行前自测试
3236	单项选择题	根据GM/T 0028《密码模块安全技术要求》，下列哪种鉴别机制不用于密码模块访问控制（）。	基于角色的鉴别	基于身份的鉴别	基于身份的多因素鉴别	基于行为方式的鉴别
3237	单项选择题	根据GM/T 0028《密码模块安全技术要求》，关于安全一级密码模块的软件/固件安全要求描述不正确的是（）。	所有的软件和固件应当确保安装前未被修改	密码边界内的所有软件和固件部件应当使用核准的完整性技术进行保护	密码边界内的所有软件或固件应当使用核准的数字签名进行保护	如果完整性测试失败，模块应当进入错误状态

3238	单项选择题	根据GM/T 0028《密码模块安全技术要求》，关于密码模块物理安全描述不正确的是（）。	安全二级增加了拆卸存迹机制的要求，以及确保无法对模块关键区域的内部操作收集信息的要求	安全三级增加了使用坚固或硬质的保形或非保形外壳的要求，要求外壳的封盖和门具有拆卸检测和响应机制，并且要求抵抗通过开口或入口的直接探测	安全四级要求具备环境失效保护（EFP），以防止错误注入攻击	当密码模块被设计成允许物理访问时，需要为维护访问接口规定安全要求。拆卸检测和拆卸响应可以代替显式的拆卸证据
3239	单项选择题	根据GM/T 0028《密码模块安全技术要求》，关于敏感安全参数管理描述不正确的是（）。	敏感安全参数包括关键安全参数和公开安全参数	采用非核准的安全功能加密的关键安全参数被认为是受保护的密文	敏感安全参数应当在模块内受保护以防止非授权的访问、使用、泄露、修改和替换	公开安全参数应当在模块内受保护以防止非授权的修改和替换
3240	单项选择题	根据GM/T 0028《密码模块安全技术要求》，以下哪个不是条件自测试的内容（）。	密码算法自测试	抗能量分析攻击自测试	配对一致性测试	软件/固件加载测试
3241	单项选择题	根据GM/T 0028《密码模块安全技术要求》，以下哪个不是生命周期保障要求的内容（）。	需求分析	配置管理	设计	配送和操作
3242	单项选择题	GB/T 39786《信息安全技术 信息系统密码应用基本要求》规定，对于密码应用第三级信息系统，应（）对密码应用安全管理制度和操作规程的合理性和适用性进行论证和审定。	不定期	定期	随时	按需
3243	单项选择题	下列选项中不属于GB/T 39786《信息安全技术 信息系统密码应基本要求》中管理制度方面相关要求的是（）。	应具备密码应用安全管理制度,包括密码人员管理、密钥管理、建设运行、应急处置、密码软硬件及介质管理等制度	应根据密码应用方案建立相应密钥管理规则	应对密码厂商相关人员执行的日常管理操作建立操作规程	应具有密码应用操作规程的相关执行记录并妥善保存

3244	单项选择题	对于密码应用第二级及以下信息系统的密钥管理策略，根据GB/T 39786《信息安全技术 信息系统密码应用基本要求》以下说法正确的是（ ）。	无需制定密钥管理策略	应根据密码应用方案，确定系统涉及的密钥种类、体系及其生命周期环节	由于信息系统的密码应用要求不高，密钥管理策略可以只涉及密钥生成环节，不必涉及其他环节	可以只针对应用和数据安全涉及的密钥制定管理策略，而忽略其他层面的密钥管理
3245	单项选择题	关于信息系统的应用和数据层面的密钥体系，根据GB/T 39786《信息安全技术 信息系统密码应用基本要求》，以下说法正确的是（ ）。	由业务系统根据密码应用需求在密码应用方案中明确，并在密码应用实施中落实	由数字证书认证系统提供	由密钥管理系统提供	由多类密码设备分别提供
3246	单项选择题	根据GB/T 39786《信息安全技术 信息系统密码应用基本要求》，关于密钥分发，以下说法错误的是（ ）。	密钥分发时要注意抗截取、篡改、假冒等攻击,保证密钥的机密性、完整性	密钥分发是密钥从一个密码产品传递到另一个密码产品的过程	密钥分发时要注意保证分发者、接收者身份的真实性	密钥分发只能通过人工方式进行
3247	单项选择题	GB/T 39786《信息安全技术 信息系统密码应用基本要求》规定，对于密码应用第三级信息系统，应建立密码应用岗位责任制度，对关键岗位建立（ ）机制。	专人专管	多人共管	多人单管	专人共管
3248	单项选择题	GB/T 39786《信息安全技术 信息系统密码应用基本要求》规定，对于密码应用第四级信息系统，应建立密码应用岗位责任制度，关键安全岗位应由（ ）员工担任。	上级	本机构	下级	密码厂商
3249	单项选择题	根据GB/T 39786《信息安全技术 信息系统密码应用基本要求》，对于密码应用第三级信息系统，（ ）采用密码技术保证系统资源访问控制信息的完整性。	应	宜	可	以上都不是

3250	单项选择题	根据GB/T 39786《信息安全技术 信息系统密码应用基本要求》，对于密码应用第三级信息系统，远程管理设备时，（ ）采用密码技术保证远程管理通道安全。	应	宜	可	以上都不是
3251	单项选择题	根据GB/T 39786《信息安全技术 信息系统密码应用基本要求》，对于密码应用第三级信息系统所采用的密码产品，以下说法正确的是（ ）。	应达到GB/T 37092三级及以上安全级别	应达到GB/T 37092二级及以上安全级别	应达到GB/T 37092二级及以下安全级别	无需具有商密认证证书
3252	单项选择题	根据GB/T 39786《信息安全技术 信息系统密码应用基本要求》，对于设备中重要可执行程序完整性，一般未采用密码技术实现的措施是（ ）。	对重要可执行程序做代码签名，安装时验签	使用可信计算，自设备上电开始逐级做完整性度量	对重要可执行程序做CBC-MAC，安装时使用密码机做验证	在操作系统上限制不同用户的软件安装权限
3253	单项选择题	根据GB/T 39786《信息安全技术 信息系统密码应用基本要求》，对于设备日志记录完整性，以下哪种做法符合信息系统第四级密码应用要求（ ）。	直接记录日志，不做任何完整性标记	不用密码技术做完整性保护，但对日志文件做定期备份	在每条日志记入的同时，对该条日志做数字签名	不用密码技术做完整性保护，但将日志包含的数据尽可能减少，不要包含敏感数据项
3254	单项选择题	根据GB/T 39786《信息安全技术 信息系统密码应用基本要求》，对于远程管理通道的安全，以下说法正确的是（ ）。	常见的远程管理协议包括SSH、RDP等	使用HTTP协议做远程管理通道就是安全的	租用运营商网络专线做远程管理通道，一定是安全的	使用串口直连方式接入设备做配置管理，也属于安全的远程管理通道
3255	单项选择题	根据GB/T 39786《信息安全技术 信息系统密码应用基本要求》，政务信息系统需要第三方电子认证服务时，应选择（ ）。	具有电子政务电子认证服务资质的机构	在工商部门合法注册的电子认证机构	使用合规密码产品的电子认证机构	由国家机关运营的电子认证机构
3256	单项选择题	GB/T 39786《信息安全技术 信息系统密码应用基本要求》中，关于网络和通信安全层面的“安全接入认证”要求，以下说法错误的是（ ）。	是对从外部连接到内部网络的设备进行接入认证，确保接入网络的设备身份真实性	密码应用第四级的信息系统宜满足该要求	密码应用第三级的信息系统可满足该要求	能防止未授权人员冒充合法的设备管理员身份

3257	单项选择题	GB/T 39786《信息安全技术 信息系统密码应用基本要求》规定了信息系统在网络和通信安全层面的密码应用技术要求，这些要求涉及到的对象不包括（ ）。	通信的主体（通信双方）	信息系统与网络边界外建立的网络通信信道	提供通信保护功能的设备、组件和产品	应用软件
3258	单项选择题	GB/T 39786《信息安全技术 信息系统密码应用基本要求》中，在网络和通信安全层面不包括以下哪方面的要求（ ）。	对通信实体进行身份鉴别	保证通信过程中数据的完整性	通信设备日志记录的完整性	保证网络边界访问控制信息的完整性
3259	单项选择题	GB/T 39786《信息安全技术 信息系统密码应用基本要求》中，对密码应用第二级信息系统网络和通信安全层面的要求，不正确的是（ ）。	宜采用密码技术对通信实体进行身份鉴别，保证通信实体身份的真实性	宜采用密码技术保证通信过程中数据的完整性	宜采用密码技术保证通信过程中重要数据的机密性	可采用密码技术保证网络边界访问控制信息的完整性
3260	单项选择题	GB/T 39786《信息安全技术 信息系统密码应用基本要求》中，对密码应用第三级信息系统网络和通信安全层面的要求，不正确的是（ ）。	应采用密码技术对通信实体进行身份鉴别，保证通信实体身份的真实性	宜采用密码技术保证通信过程中数据的完整性	宜采用密码技术保证通信过程中重要数据的机密性	宜采用密码技术保证网络边界访问控制信息的完整性
3261	单项选择题	GB/T 39786《信息安全技术 信息系统密码应用基本要求》中，在网络和通信安全层面的要求不包括（ ）。	保证通信过程中数据的完整性	重要可执行程序的来源真实性	保证通信过程中重要数据的机密性	保证网络边界访问控制信息的完整性
3262	单项选择题	根据GB/T 39786《信息安全技术 信息系统密码应用基本要求》网络和通信安全层面的要求，以下说法不正确的是（ ）。	网络和通信安全层面主要是针对跨网络访问的通信信道，这里的跨网络访问包括从不受保护的网络区域访问被测系统	网络和通信安全层面的密码应用要求主要指利用密码技术保护网络通信链路的安全，不涉及其他层次的相关概念	在网络边界部署符合要求的 IPSec VPN 或 SSL VPN 设备，是满足网络和通信安全层面要求的通用实现方法	网络和通信安全层面要求对通信过程中的数据，进行区分语义的机密性和完整性保护
3263	单项选择题	GB/T 39786《信息安全技术 信息系统密码应用基本要求》中，网络和通信安全层面的身份鉴别用于保证（ ）。	重要区域进入人员身份的真实性	通信实体身份的真实性	登录设备的用户的身份真实性	登录业务系统的用户的身份真实性

3264	单项选择题	根据GB/T 39786《信息安全技术 信息系统密码应用基本要求》，网络和通信安全层面的身份鉴别，以下说法正确的是（ ）。	对于密码应用第三级系统，应采用密码技术对通信实体进行双向身份鉴别	身份鉴别的对象是通信实体，例如SSL VPN网关设备，而非通过网络访问信息系统的业务用户	通信实体身份真实性鉴别必须通过数字签名和验签技术实现	只要身份鉴别协议所使用的密码算法是安全的，鉴别协议本身就是安全的
3265	单项选择题	GB/T 39786《信息安全技术 信息系统密码应用基本要求》规定，密码应用（ ）及以上信息系统，应采用密码技术保证通信过程中重要数据的机密性。	第一级	第二级	第三级	第四级
3266	单项选择题	根据GB/T 39786-2021《信息安全技术 信息系统密码应用基本要求》，以下哪种密码算法，不能满足网络和通信安全层面“采用密码技术保证通信数据完整性”的要求。（ ）	HMAC-SM3	SM4-GCM	SM4-CTR	SM2签名算法
3267	单项选择题	GB/T 39786《信息安全技术 信息系统密码应用基本要求》规定，密码应用第三级的信息系统，宜采用密码技术保证电子门禁系统（ ）。	进出记录数据的存储机密性	电子门禁系统管理员的身份真实性	进出记录数据的存储完整性	电子门禁系统固件的存储完整性
3268	单项选择题	GB/T 39786《信息安全技术 信息系统密码应用基本要求》规定，密码应用（ ）信息系统，宜采用密码技术保证电子门禁系统进出记录数据的存储完整性。	第一级	第二级	第三级	第四级
3269	单项选择题	以下哪项不属于GB/T 39786《信息安全技术 信息系统密码应用基本要求》中物理和环境安全层面中的重要区域（ ）。	被测信息系统所在的IDC机房	被测信息系统终端用户所在的办公室	被测信息系统所在的云服务提供商机房	被测信息系统所在的物理机房
3270	单项选择题	GB/T 39786《信息安全技术 信息系统密码应用基本要求》物理和环境安全层面的身份鉴别，用于保证（ ）。	重要区域进入人员身份的真实性	视频监控系统管理员的身份真实性	电子门禁系统管理员的身份真实性	计算机终端用户的身份真实性

3271	单项选择题	GB/T 39786《信息安全技术 信息系统密码应用基本要求》规定，密码应用（ ）信息系统，宜采用密码技术进行物理访问身份鉴别，保证重要区域进入人员身份的真实性。	第一级	第二级	第三级	第四级
3272	单项选择题	GB/T 39786《信息安全技术 信息系统密码应用基本要求》中，采用密码技术保证视频监控音像记录数据的（ ）。	存储完整性	存储机密性	传输完整性	传输机密性
3273	单项选择题	GB/T 39786《信息安全技术 信息系统密码应用基本要求》中，密码应用第三级信息系统，（ ）采用密码技术保证视频监控音像记录数据的存储完整性。	应	宜	可	无要求
3274	单项选择题	根据GB/T 39786《信息安全技术 信息系统密码应用基本要求》，对于密码应用第二级信息系统的应急处置，以下哪种说法是正确的（ ）。	可根据密码产品提供的安全策略，由用户自主处置密码应用安全事件	应制定密码应用应急策略，做好应急资源准备，当密码应用安全事件发生时，按照应急处置措施结合实际情况及时处置	应制定密码应用应急策略，做好应急资源准备，当密码应用安全事件发生时，应立即启动应急处置措施，结合实际情况及时处置	以上都不对
3275	单项选择题	根据GB/T 39786《信息安全技术 信息系统密码应用基本要求》，对于密码应用第三级及以上信息系统的应急处置，以下哪种说法是正确的（ ）。	可根据密码产品提供的安全策略，由用户自主处置密码应用安全事件	应制定密码应用应急策略，做好应急资源准备，当密码应用安全事件发生时，应等待上级批准后再实施处置	应制定密码应用应急策略，做好应急资源准备，当密码应用安全事件发生时，应立即启动应急处置措施，结合实际情况及时处置	以上都不对

3276	单项选择题	根据GB/T 39786《信息安全技术 信息系统密码应用基本要求》，对于密码应用第三级信息系统的应急处置，以下说法正确的是（ ）。	密码应用安全事件发生后，不强制要求向信息系统主管部门或属地密码管理部门进行报告	密码应用安全事件发生后，应及时向信息系统主管部门进行报告	密码应用安全事件发生后，应及时向信息系统主管部门及归属的密码管理部门进行报告	以上都不对
3277	单项选择题	根据GB/T 39786《信息安全技术 信息系统密码应用基本要求》，对于密码应用第四级信息系统的应急处置，以下说法正确的是（ ）。	密码应用安全事件发生后，不强制要求向信息系统主管部门或属地密码管理部门进行报告	密码应用安全事件发生后，应及时向信息系统主管部门进行报告	密码应用安全事件发生后，应及时向信息系统主管部门及归属的密码管理部门进行报告	以上都不对
3278	单项选择题	根据GB/T 39786《信息安全技术 信息系统密码应用基本要求》，对于密码应用第二级信息系统的应急处置情况报告，以下说法正确的是（ ）。	事件处置完成后，不强制要求向信息系统主管部门及归属的密码管理部门报告事件发生情况及处置情况	事件处置完成后，应及时向信息系统主管部门报告事件发生情况及处置情况，但不必向归属的密码管理部门报告	事件处置完成后，应及时向归属的密码管理部门报告事件发生情况及处置情况，但不必向信息系统主管部门报告	事件处置完成后，应及时向信息系统主管部门及归属的密码管理部门报告事件发生情况及处置情况
3279	单项选择题	根据GB/T 39786《信息安全技术 信息系统密码应用基本要求》，对于密码应用第三级信息系统的应急处置情况报告，以下说法正确的是（ ）。	事件处置完成后，不强制要求向信息系统主管部门及归属的密码管理部门报告事件发生情况及处置情况	事件处置完成后，应及时向信息系统主管部门报告事件发生情况及处置情况，但不必向归属的密码管理部门报告	事件处置完成后，应及时向归属的密码管理部门报告事件发生情况及处置情况，但不必向信息系统主管部门报告	事件处置完成后，应及时向信息系统主管部门及归属的密码管理部门报告事件发生情况及处置情况
3280	单项选择题	GB/T 39786《信息安全技术 信息系统密码应用基本要求》中，应用和数据安全层面的身份鉴别用于保证（ ）。	重要区域进入人员身份的真实性	通信实体身份的真实性	登录设备的用户的身份真实性	登录业务系统的用户的身份真实性

3281	单项选择题	根据GB/T 39786《信息安全技术 信息系统密码应用基本要求》，以下可用于应用和数据安全层面身份鉴别保护的密码产品是（ ）。	IPSec VPN设备	智能密码钥匙	电子文件密码应用系统	电子门禁系统
3282	单项选择题	GB/T 39786《信息安全技术 信息系统密码应用基本要求》规定，信息系统第四级密码应用要求应用和数据安全层面（ ）采用密码技术保证信息系统应用的访问控制信息的完整性。	应	宜	可	须
3283	单项选择题	GB/T 39786《信息安全技术 信息系统密码应用基本要求》规定，信息系统第四级密码应用要求应用和数据安全层面（ ）采用密码技术保证信息系统应用的重要信息资源安全标记的完整性。	应	宜	可	须
3284	单项选择题	GB/T 39786《信息安全技术 信息系统密码应用基本要求》规定，信息系统第三级密码应用要求应用和数据安全层面（ ）采用密码技术对登录用户进行身份鉴别，保证应用系统用户身份的真实性。	应	宜	可	须
3285	单项选择题	GB/T 39786《信息安全技术 信息系统密码应用基本要求》规定，信息系统第三级密码应用要求应用和数据安全层面（ ）采用密码技术保证信息系统应用的访问控制信息的完整性。	应	宜	可	须
3286	单项选择题	GB/T 39786《信息安全技术 信息系统密码应用基本要求》规定，信息系统第三级密码应用要求应用和数据安全层面（ ）采用密码技术保证信息系统应用的重要信息资源安全标记的完整性。	应	宜	可	须

3287	单项选择题	GB/T 39786《信息安全技术 信息系统密码应用基本要求》规定，信息系统第三级密码应用要求应用和数据安全层面（ ）采用密码技术保证信息系统应用的重要数据在传输过程中的机密性。	应	宜	可	须
3288	单项选择题	GB/T 39786《信息安全技术 信息系统密码应用基本要求》规定，信息系统第三级密码应用要求应用和数据安全层面（ ）采用密码技术保证信息系统应用的重要数据在存储过程中的机密性。	应	宜	可	须
3289	单项选择题	GB/T 39786《信息安全技术 信息系统密码应用基本要求》规定，信息系统第三级密码应用要求应用和数据安全层面（ ）采用密码技术保证信息系统应用的重要数据在传输过程中的完整性。	应	宜	可	须
3290	单项选择题	GB/T 39786《信息安全技术 信息系统密码应用基本要求》规定，信息系统第三级密码应用要求应用和数据安全层面（ ）采用密码技术保证信息系统应用的重要数据在存储过程中的完整性。	应	宜	可	须
3291	单项选择题	GB/T 39786《信息安全技术 信息系统密码应用基本要求》规定，信息系统第三级密码应用要求应用和数据安全层面，在可能涉及法律责任认定的应用中，（ ）采用密码技术提供数据原发证据和数据接收证据，实现数据原发行为的不可否认性和数据接收行为的不可否认性。	应	宜	可	须
3292	单项选择题	GB/T 39786《信息安全技术 信息系统密码应用基本要求》中，应用和数据安全层面要求“采用密码技术对登录用户进行身份鉴别，保证应用系统用户身份的真实性”中用户指的是()。	所有登录设备的实体	所有登录应用进行操作的实体	设备管理员	应用管理员

3293	单项选择题	GB/T 39786《信息安全技术 信息系统密码应用基本要求》规定，在应用和数据安全层面，信息系统第三级密码应用中要求采用的密码产品，应达到GB/T 37092（ ）及以上安全要求。	第一级	第二级	第三级	第四级
3294	单项选择题	GB/T 39786《信息安全技术 信息系统密码应用基本要求》规定，在应用和数据安全层面，信息系统第四级密码应用中要求采用的密码产品，应达到GB/T 37092（ ）及以上安全要求。	第一级	第二级	第三级	第四级
3295	单项选择题	以下哪个措施满足GB/T 39786《信息安全技术 信息系统密码应用基本要求》中应用和数据安全层面的相关要求（ ）。	用户将智能密码钥匙中的数字证书的序列号发送给应用系统，由应用系统在后台数据库比对，如比对成功、证书在有效期内，则身份鉴别通过	利用服务器密码机等设备对应用系统指定的重要数据，使用常数12345678作为密钥，SM4加密和计算HMAC_SM3消息鉴别码后传输，实现对重要数据（在应用和数据安全层面）传输过程中的机密性和完整性保护。	利用开源密码库内置的密码功能，对重要数据进行加密签名后存储在数据库中，实现对重要数据在存储过程中的机密性和完整性保护。	使用依法设立的第三方电子认证机构提供数字证书服务，使用具有商密产品认证证书的安全电子签章系统和时间戳服务器，来对可能涉及法律责任认定的数据原发、接收行为的不可否认性进行保护。
3296	单项选择题	下列关于GB/T 39786《信息安全技术 信息系统密码应用基本要求》应用和数据安全层面，对密码应用第三级信息系统相关指标要求说法正确的是（ ）。	可只对重要的登录用户进行身份鉴别，保证其身份的真实性	任何数据，都必须做到存储加密，否则构成高风险	任何数据，都必须要采用密码技术保证存储过程中的完整性，否则构成高风险	“应采用密码技术保证信息系统应用的访问控制信息的完整性”是GB/T 39786标准中仅对四级信息系统的要求

3297	单项选择题	根据GB/T 39786《信息安全技术 信息系统密码应用基本要求》，测评过程中，对于信息系统用户通过智能密码钥匙对电子数据做数字信封加密，并通过信息系统浏览器前端页面上传，属于（ ）层面的测评的内容。	网络和通信安全	物理和环境安全	应用和数据安全	设备和计算安全
3298	单项选择题	GB/T 39786《信息安全技术 信息系统密码应用基本要求》中，在应用和数据安全层面的“重要数据传输完整性”一般无法通过部署（ ）密码设备来实现。	IPSec VPN设备	智能密码钥匙	签名验签服务器	服务器密码机
3299	单项选择题	GB/T 39786《信息安全技术 信息系统密码应用基本要求》中，在应用和数据安全层面的“不可否认性”可通过部署（ ）密码设备来实现。	动态令牌认证系统	安全电子签章系统	对称密钥管理系统	密码键盘
3300	单项选择题	根据GB/T 39786《信息安全技术 信息系统密码应用基本要求》，对于面向电子政务领域提供电子认证服务的第三方电子认证机构，必须具备的资质有（ ）。	密码应用安全性测评资质	涉密信息系统集成资质	电子认证密码使用许可证	电子政务电子认证服务资质
3301	多项选择题	GB/T 39786《信息安全技术 信息系统密码应用基本要求》规定，管理制度方面密码应用第一级到第四级信息系统均应遵守的指标是（ ）。	具备密码应用安全管理制度	建立密钥管理规则	建立操作规程	定期修订安全管理制度
3302	多项选择题	GB/T 39786《信息安全技术 信息系统密码应用基本要求》要求信息系统应具备密码应用安全管理制度，包括（ ）。	密码人员管理制度	密钥管理制度	建设运行制度	应急处置制度
3303	多项选择题	GB/T 39786《信息安全技术 信息系统密码应用基本要求》要求信息系统应具备密码应用安全管理制度，包括（ ）。	密钥管理制度	密码软硬件及介质管理制度	工作秘密信息管理制度	应急处置制度
3304	多项选择题	GB/T 39786《信息安全技术 信息系统密码应用基本要求》规定，密码应用第二级及以上信息系统应对（ ）人员或（ ）人员执行的日常管理操作建立操作规程。	密码厂商	管理	操作	检查

3305	多项选择题	GB/T 39786《信息安全技术 信息系统密码应用基本要求》三级及以上要求信息系统应明确相关密码应用安全（ ）和（ ）的发布流程并进行版本控制。	管理制度	密码应用方案	操作规程	密码应用建设方案
3306	多项选择题	GB/T 39786《信息安全技术 信息系统密码应用基本要求》 中，关于安全管理方面的要求包括（ ）等内容。	管理制度	人员管理	资金管理	应急处置
3307	多项选择题	以下属于GB/T 39786《信息安全技术 信息系统密码应用基本要求》信息系统密码应用第二级及以上管理制度方面的要求是（ ）。	具备密码应用安全管理制度	建立操作规程	建立密码应用岗位责任制度	建立上岗人员培训制度
3308	多项选择题	根据GB/T 39786《信息安全技术 信息系统密码应用基本要求》，对于数据资产的分类分级和“重要数据”的确定，以下说法正确的是（ ）。	如果有适用的国家、行业或团体数据分级分类标准，可参考该标准	对于重要数据，必须针对其传输、存储等生命周期过程中的机密性、完整性、不可否认性安全特性都采取密码措施予以保护，否则将面临高风险	数据资产的分级，是建立在风险评估基础之上的	数据的分类分级，可以脱离信息系统的具体业务，只按照领导的意愿来做
3309	多项选择题	根据GB/T 39786《信息安全技术 信息系统密码应用基本要求》，对于密码应用第三级信息系统，以下说法正确的是（ ）。	所有技术层面的完整性要求都是“宜”	所有技术层面的身份鉴别要求都是“应”	所有技术层面的机密性要求都是“应”	所有技术层面所采用的密码产品，都应达到GB/T 37092二级及以上
3310	多项选择题	根据GB/T 39786《信息安全技术 信息系统密码应用基本要求》，在编制密码应用方案时，以下要识别的信息系统总体状况的有（ ）。	系统架构与网络拓扑	承载的业务情况	软件与硬件组成	等保定级情况
3311	多项选择题	根据GB/T 39786《信息安全技术 信息系统密码应用基本要求》，在编制密码应用方案时，要了解的信息管理机制情况有（ ）。	管理机构	人员角色	管理职责	现有安全策略

3312	多项选择题	根据GB/T 39786《信息安全技术 信息系统密码应用基本要求》，密钥安全管理策略应涵盖（ ）。	所有密钥的明文数值	密钥种类	各密钥生命周期环节	每个密钥在各生命周期环节的保护策略
3313	多项选择题	根据GB/T 39786《信息安全技术 信息系统密码应用基本要求》，对于密钥安全管理策略中关于密钥生成的策略，以下安全的方式有（ ）。	将服务器的CPU序列号作为密钥	在合规的密码产品内部用随机数发生器生成	两个合规的密码产品通过标准的密钥协商协议生成	通过合规的密码产品计算信息系统主程序的杂凑值，作为密钥
3314	多项选择题	根据GB/T 39786《信息安全技术 信息系统密码应用基本要求》，对于密钥安全管理策略中关于密钥的分发，要注意抵抗的攻击有（ ）。	抗截取	抗篡改	抗假冒	抗断网
3315	多项选择题	根据GB/T 39786《信息安全技术 信息系统密码应用基本要求》，对于公钥证书的撤销，以下说法正确的是（ ）。	撤销后的密钥不再具备使用效力	公钥证书撤销后，还需要再对其所含公钥执行撤销	公钥证书到期后，其公钥自然撤销	公钥证书在CRL中出现，即视为已撤销
3316	多项选择题	根据GB/T 39786《信息安全技术 信息系统密码应用基本要求》，对于密码应用实施，以下说法正确的是（ ）。	考虑到信息系统的具体情况，可以不按照已通过评估的密码应用方案实施建设	密码应用的实施，由密码应用安全性评估机构负责	应按照已经通过评估的密码应用方案实施建设	密码应用实施由信息系统责任单位及其委托的系统集成商、密码厂商负责
3317	多项选择题	根据GB/T 39786《信息安全技术 信息系统密码应用基本要求》，对于已投入运行的密码应用第三级以上信息系统，以下说法正确的是（ ）。	可以不再定期开展密码应用安全性评估	应严格执行既定的密码应用安全管理制度	应定期开展密码应用安全性评估	应定期开展攻防对抗演习

3318	多项选择题	根据GB/T 39786《信息安全技术 信息系统密码应用基本要求》，关于密钥管理，以下说法正确的是（ ）。	密钥分发时要注意抗截取、篡改、假冒等攻击，保证密钥的机密性、完整性	密钥在符合 GB/T 37092的密码产品中产生是十分必要的，产生的同时可在密码产品中记录密钥关联信息，包括密钥种类、长度、拥有者、使用起始时间、使用终止时间等	密钥不以明文方式存储在密码产品外部是十分必要的，应采取严格的安全防护措施，防止密钥 被非授权的访问或篡改	公钥可以以明文方式在密码产品外存储、传递和使用，无需采取任何防护措施
3319	多项选择题	根据GB/T 39786《信息安全技术 信息系统密码应用基本要求》，密钥的生存周期可能包括的环节有（ ）。	密钥的产生、分发	密钥的存储、使用、更新	密钥的归档、撤销	密钥的备份、恢复、销毁
3320	多项选择题	根据GB/T 39786《信息安全技术 信息系统密码应用基本要求》，关于密钥备份，以下说法正确的是（ ）。	对于需要备份的密钥，采用安全的备份机制对密钥进行备份是必要的，以确保备份密钥的机密性和完整性	密钥备份行为是审计涉及的范围,有必要生成审计信息，包括备份的主体、备份的时间等	密钥备份的主要目的是保护密钥的可用性，作为密钥存储的补充以防止密钥的意外损坏	密钥备份时一般将备份的密钥存储在外部存储介质中，需要有安全机制保证仅有密钥拥有者才能恢复出密钥明文
3321	多项选择题	根据GB/T 39786《信息安全技术 信息系统密码应用基本要求》，关于密钥存储，以下说法正确的是（ ）。	密钥不以明文方式存储在密码产品外部是十分必要的，应采取严格的安全防护措施，防止密钥 被非授权的访问或篡改	公钥可以以明文方式在密码产品外存储、传递和使用，但有必要采取安全防护措施,防止公钥被非授权篡改	为了保证密钥存储安全，可以将密钥存储在密码产品中，或者在对密钥进行机密性和完整性保护后，存储在通用存储设备或系统（如数据库）中	并非所有密钥都需要存储，一些临时密钥或一次一密的密钥在使用完就要立即进行销毁

3322	多项选择题	根据GB/T 39786《信息安全技术 信息系统密码应用基本要求》，关于密钥分发，以下说法正确的是（ ）。	为了节省密钥资源，一个密钥可以提供给多个不同层面的密码技术措施使用	每个密钥一般只有单一的用途，明确用途并按用途正确使用是十分必要的	有必要为密钥设定更换周期，并采取有效措施保证密钥更换时的安全性	密钥使用环节需要注意的安全问题是：使用密钥前获得授权、使用公钥证书前对其进行有效性验证、采用安全措施防止密钥的泄露和替换等
3323	多项选择题	根据GB/T 39786《信息安全技术 信息系统密码应用基本要求》，以下哪些情况需要对密钥进行更新（ ）。	密钥超过使用期限	密钥已泄露	密钥存在泄露风险	密钥已经成功分发
3324	多项选择题	根据GB/T 39786《信息安全技术 信息系统密码应用基本要求》，关于密钥备份和恢复，以下说法正确的是（ ）。	对于需要备份的密钥，采用安全的备份机制对密钥进行备份是必要的，以确保备份密钥的机密 性和完整性	密钥备份行为是审计涉及的范围,有必要生成审计信息，包括备份的主体、备份的时间等	密钥恢复可以支持用户密钥恢复和司法密钥恢复	密钥恢复行为是审计涉及的范围，有必要生成审计信息，包括恢复的主体、恢复的时间等
3325	多项选择题	根据GB/T 39786《信息安全技术 信息系统密码应用基本要求》，关于密钥使用，以下说法正确的是（ ）。	每个密钥一般只有单一的用途,明确用途并按用途正确使用是十分必要的	密钥使用环节需要注意的安全问题是：使用密钥前获得授权、使用公钥证书前对其进行有效性验证、采用安全 措施防止密钥的泄露和替换等	有必要为密钥设定更换周期，并采取有效措施保证密钥更换时的安全性	密钥生存周期管理的技术实现由密码产品提供，即便密码产品不具有商密产品认证证书，也能保证密钥的安全
3326	多项选择题	GB/T 39786《信息安全技术信息系统密码应用基本要求》在人员管理方面的（ ）指标是密码应用第三级信息系统应遵守的。	了解并遵守密码相关法律法规、密码管理制度	建立关键人员保密制度和调离制度	建立上岗人员培训制度	定期对密码应用安全岗位人员进行考核

3327	多项选择题	根据GB/T 39786《信息安全技术 信息系统密码应用基本要求》，在人员管理方面，密码应用第四级系统较第三级系统增加的要求有（ ）。	相关设备与系统的管理和使用账号不得多人共用	密钥管理员、密码安全审计员、密码操作员应由本机构的内部员工担任	密钥管理员、密码安全审计员、密码操作员应在任前对其进行背景调查	对关键岗位建立多人共管机制
3328	多项选择题	GB/T 39786《信息安全技术 信息系统密码应用基本要求》要求信息系统的相关人员应了解并遵守密码相关法律法规、密码应用安全管理制度，包括（ ）。	密码法	电子签名法	密码产品操作规程	密码设备配置说明
3329	多项选择题	根据GB/T 39786《信息安全技术 信息系统密码应用基本要求》，密码应用第三级信息系统对人员管理层面的要求包括（ ）。	具备密码应用安全管理制度	建立操作规程	建立密码应用岗位责任制度	建立上岗人员培训制度
3330	多项选择题	根据GB/T 39786《信息安全技术 信息系统密码应用基本要求》，以下哪些用户在“设备和计算安全”层面需要做身份鉴别（ ）。	数据库的审计员用户	服务器操作系统中的管理员用户	进入机房的安检人员	在OA系统上具有审批权的用户
3331	多项选择题	根据GB/T 39786《信息安全技术 信息系统密码应用基本要求》，以下基于密码技术的哪些机制可以用在对登录设备用户的身份鉴别上（ ）。	动态口令	基于数字签名的挑战响应	基于HMAC的挑战响应	基于CBC-MAC的挑战响应
3332	多项选择题	根据GB/T 39786《信息安全技术 信息系统密码应用基本要求》，在使用堡垒机作为设备管理统一入口时，以下说法正确的是（ ）。	商密产品认证目录中没有堡垒机这个类别，因此无需在意堡垒机内部密钥管理是否有风险	堡垒机与各个设备的连接通道，如果采用了密码技术，也要考虑避免使用高风险的密码算法	堡垒机如果和登录的客户端之间建立了符合TLCP的安全通道，则无需再使用密码技术对使用该客户端登录的管理员用户做身份鉴别	堡垒机与登录客户端之间的通信通道，应作为远程安全管理通道考虑，需符合远程管理通道的密码应用要求
3333	多项选择题	根据GB/T 39786《信息安全技术 信息系统密码应用基本要求》，以下可用于基于密码技术的远程管理通道安全的安全通信协议有（ ）。	SSL	TLCP	IPSec	MPLS

3334	多项选择题	根据GB/T 39786《信息安全技术 信息系统密码应用基本要求》，可用于保证重要信息资源安全标记完整性的密码技术有（ ）。	动态口令	数字信封	数字签名	消息鉴别码（MAC）
3335	多项选择题	根据GB/T 39786《信息安全技术 信息系统密码应用基本要求》，可用于保证日志记录完整性的密码技术有（ ）。	数字签名	数字信封	消息鉴别码（MAC）	动态口令
3336	多项选择题	根据GB/T 39786《信息安全技术 信息系统密码应用基本要求》，可用于保证设备中重要可执行程序完整性、重要可执行程序来源真实性的密码技术措施有（ ）。	对重要可执行程序做代码签名，安装时验签	使用可信计算，自设备上电开始逐级做完整性度量	对重要可执行程序做CBC-MAC，安装时使用密码机做验证	在操作系统上限制不同用户的软件安装权限
3337	多项选择题	根据GB/T 39786《信息安全技术 信息系统密码应用基本要求》，可以提供基于非对称密码算法的数字签名功能的密码产品有（ ）。	密码键盘	签名验签服务器	服务器密码机	智能密码钥匙
3338	多项选择题	根据GB/T 39786《信息安全技术 信息系统密码应用基本要求》，使用的密码产品需要具备商用密码产品认证证书的信息系统级别是（ ）。	第一级	第二级	第三级	第四级
3339	多项选择题	根据GB/T 39786《信息安全技术 信息系统密码应用基本要求》，属于《商用密码产品认证目录》中的密码产品种类的是（ ）。	签名验签服务器	服务器密码机	随机数发生器	云服务器密码机
3340	多项选择题	根据GB/T 39786《信息安全技术 信息系统密码应用基本要求》，对于“动态令牌”产品，以下说法正确的是（ ）。	是一种生成并显示动态口令的载体	应具备SM2数字签名功能	应与“动态令牌认证系统”搭配使用	既可基于对称密码算法来计算动态口令，也可基于密码杂凑算法来计算

3341	多项选择题	根据GB/T 39786《信息安全技术 信息系统密码应用基本要求》，关于商用密码产品检测认证，与密码应用安全性评估的关系，以下说法正确的是（）。	二者都是针对密码产品的检测	商用密码产品检测认证的认证对象是商用密码产品，而密评的对象是承载某类信息化业务的信息系统	即便一个信息系统使用的商用密码产品全都具有商用密码认证证书，也不一定能够通过密评	国外厂商研制的商用密码产品，一定无法通过商用密码产品检测并获得认证证书
3342	多项选择题	根据GB/T 39786《信息安全技术 信息系统密码应用基本要求》，关于密码服务以下说法错误的是（）。	所有密码应用等级的信息系统，其采用的密码服务均应符合法律法规的相关要求，需依法接受检测认证的，应经商用密码认证机构认证合格	只有三级及以上信息系统，采用的密码服务才应符合法律法规的相关要求，需依法接受检测认证的，应经商用密码认证机构认证合格。其他密码应用级别的信息系统可以自由选择	只要密码服务所使用的密码产品是具有商密产品认证证书的，则肯定是合规的密码服务	GB/T 39786对信息系统使用的密码服务提任何要求
3343	多项选择题	GB/T 39786《信息安全技术 信息系统密码应用基本要求》要求信息系统中使用的密码技术应遵循密码相关国家标准和行业标准，以下属于密码技术的是（）。	密码算法	密码协议	密钥管理	恶意软件检测
3344	多项选择题	以下符合GB/T 39786《信息安全技术 信息系统密码应用基本要求》通用要求中对密码算法规定的密码算法有（）。	SM4	SM9	ZUC	SM3

3345	多项选择题	根据GB/T 39786《信息安全技术 信息系统密码应用基本要求》，关于网络和通信安全层面的安全接入认证的说法，以下说法错误的有（ ）。	“安全接入认证”是对从外部连接到内部网络的设备进行接入认证，确保接入网络的设备身份真实性	密码应用第四级信息系统，应采用密码技术对从外部连接到内部网络的设备进行接入认证，确保接入设备身份的真实性	密码应用第三级信息系统，宜采用密码技术对从外部连接到内部网络的设备进行接入认证，确保接入设备身份的真实性	密码应用第二级信息系统，宜采用密码技术对从外部连接到内部网络的设备进行接入认证，确保接入设备身份的真实性
3346	多项选择题	根据GB/T 39786《信息安全技术 信息系统密码应用基本要求》，关于网络和通信安全层面的安全接入认证和身份鉴别指标的说法，正确的有（ ）。	“身份鉴别”指标适用于两个实体通过不可控的网络（比如互联网）进行通信之前进行的身份鉴别。	IPSec VPN 或者 SSL 客户端/服务器的场景，IPSec VPN 之间或者 SSL 客户端和服务端之间的鉴别都属于“身份鉴别”指标的测评范围	“安全接入认证”指标适用于设备“物理地”从外部接入信息系统的内部网络之前对设备的身份鉴别，接入后，该设备将成为信息系统内部网络的一部分	IPSec VPN 或者 SSL 客户端/服务器的场景，IPSec VPN 之间或者 SSL 客户端和服务端之间的鉴别都属于“设备接入认证”指标的测评范围
3347	多项选择题	根据GB/T 39786《信息安全技术 信息系统密码应用基本要求》，以下属于网络和通信安全层面的安全措施包括（ ）。	在网络边界部署符合要求的IPSec VPN设备	在网络边界部署符合要求的SSL VPN设备	采用密码产品对边界防护设备的访问控制信息计算 MAC 或签名后保存，以保证信息的完整性	采用HTTPS与信息系统建立安全通信通道
3348	多项选择题	根据GB/T 39786《信息安全技术 信息系统密码应用基本要求》，在网络和通信安全层面包括的要求有（ ）。	对通信实体进行身份鉴别	保证通信过程中数据的完整性	保证通信过程中重要数据的机密性	保证网络边界访问控制信息的完整性

3349	多项选择题	根据GB/T 39786《信息安全技术 信息系统密码应用基本要求》，网络和通信安全层面主要关注通信主体之间的信道安全，以下属于该层面关注的通信信道有（ ）。	PC机上运行的浏览器与服务器上运行的web服务系统之间的通信信道	移动智能终端上运行的APP与服务器上运行的应用系统之间的通信信道	服务端与服务端（例如，IPSec VPN与IPSec VPN之间）之间的通信信道	基于专网搭建的安全电子邮件传递
3350	多项选择题	根据GB/T 39786《信息安全技术 信息系统密码应用基本要求》，对密码应用第二级的信息系统网络和通信安全层面的要求，正确的是（ ）。	宜采用密码技术对通信实体进行身份鉴别，保证通信实体身份的真实性	宜采用密码技术保证通信过程中数据的完整性	宜采用密码技术保证通信过程中重要数据的机密性	可采用密码技术保证网络边界访问控制信息的完整性
3351	多项选择题	根据GB/T 39786《信息安全技术 信息系统密码应用基本要求》，对密码应用第三级的信息系统网络和通信安全层面的要求，正确的是（ ）。	应采用密码技术对通信实体进行身份鉴别，保证通信实体身份的真实性	宜采用密码技术保证通信过程中数据的完整性	宜采用密码技术保证通信过程中重要数据的机密性	宜采用密码技术保证网络边界访问控制信息的完整性
3352	多项选择题	根据GB/T 39786《信息安全技术 信息系统密码应用基本要求》，可用于网络和通信安全层面的密码产品包括（ ）。	安全电子签章系统	SSL VPN设备	IPSec VPN设备	安全浏览器
3353	多项选择题	根据GB/T 39786《信息安全技术 信息系统密码应用基本要求》，以下属于网络和通信安全层面关注的通信信道有（ ）。	被测系统与第三方电子认证服务相关系统之间的通信信道	政务外网VPN客户端与内网SSL VPN之间的通信信道	办公内网国密浏览器与后台管理系统之间的通信信道	互联网VPN客户端与运维SSL VPN之间的运维通信信道
3354	多项选择题	GB/T 39786《信息安全技术 信息系统密码应用基本要求》对网络和通信安全层面提出的要求包括（ ）。	通信实体身份的真实性	通信过程中数据的完整性、重要数据的机密性	网络边界访问控制信息的完整性	从外部连接到内部网络的设备身份的真实性
3355	多项选择题	GB/T 39786《信息安全技术 信息系统密码应用基本要求》规定了信息系统在网络和通信安全层面的密码应用技术要求，这些要求涉及到的对象包括（ ）。	通信的主体（通信双方）	信息系统与网络边界外建立的网络通信信道	提供通信保护功能的设备、和产品	提供通信保护功能的组件

3356	多项选择题	根据GB/T 39786《信息安全技术 信息系统密码应用基本要求》，密码应用第三级信息系统在网络和通信安全层面的身份鉴别，以下说法正确的是（）。	应在通信前基于密码技术对通信双方进行双向身份鉴别	使用密码技术的机密性和真实性功能来实现防截获、防假冒和防重用，保证传输过程中鉴别信息的机密性和网络设备实体身份的真实性	通信实体身份真实性鉴别必须采用数字签名技术实现	对于实体鉴别协议，要尽可能使用GB/T 15843《信息技术 安全技术 实体鉴别》中规定协议，避免由非专业人员自行设计
3357	多项选择题	根据GB/T 39786《信息安全技术 信息系统密码应用基本要求》，属于网络和通信安全层面的身份鉴别的包括（）。	网络设备对登录到设备的管理用户进行身份鉴别	SSL VPN设备之间在建立连接之前对通信双方的身份鉴别	IPSec VPN设备之间在建立连接之前对通信双方的身份进行鉴别	操作系统开机时的用户登录认证
3358	多项选择题	根据GB/T 39786《信息安全技术 信息系统密码应用基本要求》，关于网络和通信安全层面的身份鉴别的说法，正确的有（）。	通信实体之间身份鉴别可以采用 PKI 和数字签名技术实现	通信实体之间身份鉴别可以采用对称密码算法实现	通信实体之间身份鉴别可以采用带密钥的杂凑算法（HMAC）实现	当使用PKI和数字签名来实现时，由于不涉及法律责任认定，所以不一定选择第三方电子认证机构来颁发数字证书
3359	多项选择题	根据GB/T 39786《信息安全技术 信息系统密码应用基本要求》，在某条通信信道上部署IPSec VPN设备之后，通常可以满足该条信道在网络和通信安全层面的哪几项安全要求（）。	通信实体之间的身份鉴别	通信过程中重要数据的机密性	业务行为的不可否认性	通信过程中数据的完整性
3360	多项选择题	根据GB/T 39786《信息安全技术 信息系统密码应用基本要求》，在某条通信信道上部署SSL VPN设备之后，通常可以满足该条信道在网络和通信安全层面的哪几项安全要求（）。	通信实体之间的身份鉴别	通信过程中重要数据的机密性	业务行为的不可否认性	通信过程中数据的完整性

3361	多项选择题	根据GB/T 39786《信息安全技术 信息系统密码应用基本要求》，关于网络和通信安全层面保证通信过程中重要数据机密性的说法，不正确的有（）。	网络和通信安全层面对数据进行加密保护之后，应用和数据安全层面肯定无需再次加密了	网络层安全协议例如TLCP，支持对通信报文内容的解析，从而可以有选择的加密报文数据的指定部分，而其他部分不加密	在网络边界部署符合要求的IPSec VPN/SSL VPN设备，能为通信过程中的全部数据提供机密性保护	在网络边界部署符合要求的IPSec VPN/SSL VPN设备，能为通信过程中的全部数据提供完整性保护
3362	多项选择题	GB/T 39786《信息安全技术 信息系统密码应用基本要求》规定在网络和通信安全层面“采用密码技术保证网络边界访问控制信息的完整性”，以下属于网络边界访问控制信息的有（）。	IPSEC VPN网关中的访问控制列表	防火墙的访问控制列表	边界路由的访问控制列表	业务应用的数据访问控制列表
3363	多项选择题	GB/T 39786《信息安全技术 信息系统密码应用基本要求》规定在网络和通信安全层面“采用密码技术保证网络边界访问控制信息的完整性”，以下属于网络边界访问控制信息的有（）。	IPSEC VPN网关中的访问控制列表	边界防火墙的访问控制列表	边界路由的访问控制列表	SSLVPN网关中的访问控制列表
3364	多项选择题	GB/T 39786《信息安全技术 信息系统密码应用基本要求》规定在网络和通信安全层面“采用密码技术保证网络边界访问控制信息的完整性”，以下不属于网络边界访问控制信息的有（）。	服务器的管理用户访问控制列表	边界防火墙的访问控制列表	边界路由的访问控制列表	业务应用的数据访问控制列表
3365	多项选择题	GB/T 39786《信息安全技术 信息系统密码应用基本要求》规定，密码应用（）的信息系统，可采用密码技术保证电子门禁系统进出记录数据的存储完整性。	第一级	第二级	第三级	第四级
3366	多项选择题	GB/T 39786《信息安全技术 信息系统密码应用基本要求》规定，密码应用第三级的信息系统在物理和环境层面，宜采用密码技术保护的对象及特性包括（）。	身份鉴别	电子门禁记录数据存储完整性	视频监控记录数据存储完整性	电子门禁记录数据存储机密性

3367	多项选择题	以下哪些项属于GB/T 39786《信息安全技术 信息系统密码应用基本要求》中物理和环境安全层面中的重要区域（ ）。	被测信息系统所在的IDC机房	被测信息系统所在的运营商机房	被测信息系统所在的云服务提供商机房	被测信息系统所在的物理机房
3368	多项选择题	GB/T 39786《信息安全技术 信息系统密码应用基本要求》中，物理和环境安全层面的重要区域指被测信息系统所在的物理机房，具体包括（ ）。	物理机房的防火情况	物理机房的电子门禁系统	物理机房的视频监控系统	物理机房的供电情况
3369	多项选择题	GB/T 39786《信息安全技术 信息系统密码应用基本要求》规定，密码应用第四级的信息系统，物理和环境安全层面应采用密码技术保护的对象及特性包括（ ）。	物理访问身份鉴别	电子门禁记录数据存储完整性	视频监控记录数据存储完整性	电子门禁记录数据存储机密性
3370	多项选择题	以下属于GB/T 39786《信息安全技术 信息系统密码应用基本要求》中物理和环境安全层面中的重要区域的是（ ）。	被测信息系统所在的云服务提供商机房	被测信息系统所在的运营商机房	被测信息系统所有用户的办公室	被测信息系统所在的物理机房
3371	多项选择题	GB/T 39786《信息安全技术 信息系统密码应用基本要求》物理和环境安全层面提出的要求包括（ ）。	重要区域进入人员身份的真实性	视频监控音像记录数据的存储完整性	电子门禁系统进出记录数据的存储完整性	计算机终端用户的身份真实性
3372	多项选择题	GB/T 39786《信息安全技术 信息系统密码应用基本要求》规定，哪些密码应用等级的信息系统，宜采用密码技术进行物理访问身份鉴别，保证重要区域进入人员身份的真实性（ ）。	第一级	第二级	第三级	第四级
3373	多项选择题	根据GB/T 39786《信息安全技术 信息系统密码应用基本要求》，以下可用于保护信息系统物理和环境层面安全的密码产品包括（ ）。	符合GM/T 0036《采用非接触卡的门禁系统密码应用指南》的电子门禁系统	符合GM/T 0024《SSL VPN技术规范》的SSL VPN产品	符合 GM/T 0022《IPSec VPN技术规范》的IP VPN产品	符合GM/T 0030《服务器密码机技术规范》的服务器密码机产品
3374	多项选择题	GB/T 39786《信息安全技术 信息系统密码应用基本要求》在采用密码技术保证视频监控音像记录数据的存储完整性方面，对哪些密码应用等级的信息系统未作要求（ ）。	第一级	第二级	第三级	第四级

3375	多项选择题	根据GB/T 39786《信息安全技术 信息系统密码应用基本要求》，对哪些密码应用等级的信息系统责任单位，应制定密码应用应急策略（ ）。	第一级	第二级	第三级	第四级
3376	多项选择题	根据GB/T 39786《信息安全技术 信息系统密码应用基本要求》，对哪些密码应用等级的信息系统责任单位，当密码应用安全事件发生时，应立即启动应急处置措施（ ）。	第一级	第二级	第三级	第四级
3377	多项选择题	根据GB/T 39786《信息安全技术 信息系统密码应用基本要求》，密码应用第三级信息系统责任单位，应（ ）。	制定密码应用应急策略	做好应急资源准备	密码应用安全事件发生时，立即启动应急处置措施	为信息系统密码应用购买商业保险
3378	多项选择题	根据GB/T 39786《信息安全技术 信息系统密码应用基本要求》，以下对于应急策略，说法正确的是（ ）。	信息系统责任单位必须把密码应用应急策略单独作为一份文件颁布，不能合并在已有的网络安全应急策略文件之内	对于密码应用第一级信息系统，不强制要求制定密码应用应急策略	应急策略制定完成后，也要定期复查其适用性，有条件的话可以组织定期演练	应急策略制定完成就应该束之高阁，不再理会
3379	多项选择题	根据GB/T 39786《信息安全技术 信息系统密码应用基本要求》，哪些密码应用等级信息系统责任单位，在密码应用安全事件发生后，应及时向信息系统主管部门进行报告。（ ）	第一级	第二级	第三级	第四级
3380	多项选择题	根据GB/T 39786《信息安全技术 信息系统密码应用基本要求》，哪些密码应用等级信息系统责任单位，在密码应用安全事件发生后，不强制要求向信息系统主管部门或所属的密码管理部门进行报告。（ ）	第一级	第二级	第三级	第四级

3381	多项选择题	根据GB/T 39786《信息安全技术 信息系统密码应用基本要求》，当密码设备的随机数发生器故障失效时，以下说法正确的是（ ）。	不会影响使用已有对称密钥做SM4-ECB加密的安全性	不会影响使用已有私钥做SM2数字签名的安全性	不会影响使用已有公钥做SM2数字信封的安全性	不会影响SM3杂凑运算的安全性
3382	多项选择题	根据GB/T 39786《信息安全技术 信息系统密码应用基本要求》，当使用第三方电子认证机构提供数字证书服务时，如果信息系统的签名私钥泄露，以下应急处置措施得当的是（ ）。	立即向电子认证机构申请证书撤销	立即暂停业务中数字签名功能。如因此导致业务中断，考虑暂时转为线下纸质件和手写签名或盖章	尽快组织人员，排查发生私钥泄露的环节和原因，并评估出现更多私钥泄露的可能性	如果原因是工作人员误操作导致，应考虑适时修订相关管理制度，细化操作规程并严格监督执行
3383	多项选择题	根据GB/T 39786《信息安全技术 信息系统密码应用基本要求》，哪些密码应用等级信息系统责任单位，在密码应用安全事件处置完成后，应及时向信息系统主管部门和归属的密码管理部门报告事件发生情况及处置情况（ ）。	第一级	第二级	第三级	第四级
3384	多项选择题	根据GB/T 39786《信息安全技术 信息系统密码应用基本要求》，哪些密码应用等级信息系统责任单位，在密码应用安全事件处置完成后，不强制要求向信息系统主管部门或归属的密码管理部门报告事件发生情况及处置情况（ ）。	第一级	第二级	第三级	第四级
3385	多项选择题	根据GB/T 39786《信息安全技术 信息系统密码应用基本要求》，对于密码应用第三级及以上信息系统责任单位，在密码应用安全事件处置完成后，应及时向哪些部门报告事件发生情况及处置情况（ ）。	外国驻华机构	信息系统主管部门	归属的密码管理部门	国务院
3386	多项选择题	以下属于GB/T 39786《信息安全技术 信息系统密码应用基本要求》应用和数据安全层面保护的对象是（ ）。	应用用户的身份鉴别信息	应用访问控制信息	重要业务数据	操作行为

3387	多项选择题	GB/T 39786《信息安全技术 信息系统密码应用基本要求》中，在应用和数据安全层面，对（ ）做了完整性保护要求。	应用的访问控制信息	应用的重要信息资源安全标记	所有业务数据	应用的重要业务数据
3388	多项选择题	根据GB/T 39786《信息安全技术 信息系统密码应用基本要求》，下列属于采用密码技术实现对用户进行身份鉴别的是（ ）。	智能密码钥匙	短信验证码	动态令牌	ID卡
3389	多项选择题	根据GB/T 39786《信息安全技术 信息系统密码应用基本要求》，使用以下（ ）措施可安全、合规地满足应用和数据安全中的“重要数据存储完整性”指标的要求。	使用SM3算法计算杂凑值	使用SHA-1和RSA-1024算法计算签名值	使用HMAC-SM3算法计算消息鉴别码	使用SM3和SM2算法计算签名值
3390	多项选择题	以下属于GB/T 39786《信息安全技术 信息系统密码应用基本要求》应用和数据安全层面访问控制信息的是（ ）。	应用管理员权限	操作系统访问控制信息	本单位应用用户读写权限	防火墙访问控制信息
3391	多项选择题	根据GB/T 39786《信息安全技术 信息系统密码应用基本要求》，关于应用和数据安全层面的访问控制信息完整性的说法，正确的有（ ）。	应用访问控制信息一般存在应用的数据库中	密码应用二级系统“宜采用密码技术保证信息系统应用的访问控制信息的完整性”	密码应用三级系统“宜采用密码技术保证信息系统应用的访问控制信息的完整性”	密码应用四级系统“应采用密码技术保证信息系统应用的访问控制信息的完整性”
3392	多项选择题	根据GB/T 39786《信息安全技术信息系统密码应用基本要求》，以下属于应用和数据安全层面安全措施的是（ ）。	在移动终端上使用协同签名密码模块登录APP后台信息系统	通过安全认证网关对登录用户的身份进行鉴别	在PC客户端上调用智能密码钥匙对数据签名后传输	采用密码产品对边界防护设备的访问控制信息计算 MAC 或签名后保存，以保证其完整性
3393	多项选择题	根据GB/T 39786《信息安全技术信息系统密码应用基本要求》，在应用和数据安全层面包括的要求有（ ）。	对通信实体进行身份鉴别	保证在通信过程中应用重要数据的完整性	保证在通信过程中应用重要数据的机密性	保证网络边界访问控制信息的完整性

3394	多项选择题	根据GB/T 39786《信息安全技术信息系统密码应用基本要求》，对密码应用第二级的信息系统应用和数据安全层面的要求，正确的是（ ）。	宜采用密码技术对登录用户进行身份鉴别，保证应用系统用户身份的真实性	可采用密码技术保证信息系统应用的访问控制信息的完整性	可采用密码技术保证信息系统应用的重要信息资源安全标记的完整性	宜采用密码技术保证信息系统应用的重要数据在存储过程中的机密性
3395	多项选择题	根据GB/T 39786《信息安全技术信息系统密码应用基本要求》，对密码应用第三级的信息系统应用和数据安全层面的要求，正确的是（ ）。	应采用密码技术对登录用户进行身份鉴别，保证应用系统用户身份的真实性	宜采用密码技术保证信息系统应用的访问控制信息的完整性	应采用密码技术保证信息系统应用的重要数据在存储过程中的机密性	应采用密码技术保证信息系统应用的重要数据在存储过程中的完整性
3396	多项选择题	根据GB/T 39786《信息安全技术信息系统密码应用基本要求》，可用于应用和数据安全层面保护的技术措施包括（ ）。	协同签名密码模块	服务器密码机	签名验签服务器	数字证书认证系统
3397	多项选择题	根据GB/T 39786《信息安全技术信息系统密码应用基本要求》，关于应用和数据安全层面保证重要数据传输机密性的说法，不正确的有（ ）。	若网络和通信安全层面对数据进行加密保护之后，应用和数据安全层面无需再次加密保护	责任单位如果声明信息系统没有重要数据，则密评机构在测评时，直接将相关指标标记为不适用	在网络边界部署符合要求的IPSec VPN/SSL VPN设备，能为数据提供全链路的机密性保护	重要数据传输机密性必须使用非对称加密来实现
3398	多项选择题	GB/T 39786《信息安全技术 信息系统密码应用基本要求》规定，密码应用第三级的信息系统，在应用和数据安全层面，宜采用密码技术保护的对象及特性有（ ）。	重要数据存储机密性	访问控制信息完整性	重要数据传输完整性	重要数据存储完整性
3399	多项选择题	GB/T 39786《信息安全技术 信息系统密码应用基本要求》规定，密码应用（ ）信息系统，宜/应采用密码技术保证信息系统应用的重要信息资源安全标记的完整性。	第一级	第二级	第三级	第四级
3400	多项选择题	GB/T 39786《信息安全技术 信息系统密码应用基本要求》中，密码应用第二级信息系统没有明确要求的有（ ）。	访问控制信息完整性	重要信息资源安全标记完整性	重要数据存储完整性	不可否认性

3401	多项选择题	GB/T 39786《信息安全技术 信息系统密码应用基本要求》在不可否认性方面，对哪些密码应用等级的信息系统未作要求（ ）。	第一级	第二级	第三级	第四级
3402	多项选择题	GB/T 39786《信息安全技术 信息系统密码应用基本要求》规定，密码应用第三级的信息系统，在应用和数据安全层面，哪些密码机制的实现应使用GB/T 37092二级及以上密码产品（ ）。	身份鉴别	重要数据存储机密性	访问控制信息完整性	重要数据存储完整性
3403	多项选择题	GB/T 39786《信息安全技术 信息系统密码应用基本要求》在应用和数据安全层面身份鉴别指标保护的对象可能是（ ）。	登录OA系统的用户	登录密码机的设备管理员	登录即时通信系统的用户	登录网上银行的用户
3404	多项选择题	根据GB/T 39786《信息安全技术 信息系统密码应用基本要求》，重要数据传输时在以下（ ）链路不会在网络和通信安全层面、应用和数据安全层面发生重叠。	发送方客户端到其网络出口IPSec VPN之前	发送方IPSec VPN与接收方IPSec VPN之间	重要数据在ESP协议保护下传输时	接收方网络出口IPSec VPN到应用服务器
3405	多项选择题	根据GB/T 39786《信息安全技术 信息系统密码应用基本要求》，在应用中，可基于（ ）实现重要行为的不可否认性。	签名验签服务器	时间戳服务器	证书认证系统	电子门禁系统
3406	多项选择题	根据GB/T 39786《信息安全技术信息系统密码应用基本要求》，可能用于应用和数据安全层面保护的密码产品包括（ ）。	智能密码钥匙	IPSec VPN网关	签名验签服务器	数字证书认证系统
3407	判断题	GB/T 39786《信息安全技术 信息系统密码应用基本要求》规定，所有密码应用等级信息系统均应根据密码应用方案建立相应密钥管理规则。	正确	错误		
3408	判断题	GB/T 39786《信息安全技术 信息系统密码应用基本要求》规定，所有密码应用等级信息系统均应对管理人员或操作人员执行的日常管理操作建立操作规程。	正确	错误		

3409	判断题	GB/T 39786《信息安全技术 信息系统密码应用基本要求》规定，密码应用第三级及以上信息系统，应定期对密码应用安全管理制度和操作规程的合理性和适用性进行论证和审定,对存在不足或需要改进之处进行修订。	正确	错误		
3410	判断题	GB/T 39786《信息安全技术 信息系统密码应用基本要求》规定，密码应用第二级及以上信息系统，应定期对密码应用安全管理制度和操作规程的合理性和适用性进行论证和审定,对存在不足或需要改进之处进行修订。	正确	错误		
3411	判断题	GB/T 39786《信息安全技术 信息系统密码应用基本要求》规定，密码应用第三级及以上信息系统，应具有密码应用操作规程的相关执行记录并妥善保存。	正确	错误		
3412	判断题	根据GB/T 39786《信息安全技术 信息系统密码应用基本要求》，在密码应用第三级及以上信息系统运行过程中，应严格执行既定的密码应用安全管理制度，应定期开展密码应用安全性评估及攻防对抗演习，并根据评估结果进行整改。	正确	错误		
3413	判断题	制定密码应用方案时，应严格按照GB/T 39786《信息安全技术 信息系统密码应用基本要求》相应等级的每一条密码应用要求进行设计，有任何一条要求不符合，则方案整体必然不符合。	正确	错误		
3414	判断题	根据GB/T 39786《信息安全技术 信息系统密码应用基本要求》，当信息系统发生大规模改造时，由于改造前已经通过了密码应用安全性评估，所以改造后可以不再进行密码应用安全性评估，直接投入运行。	正确	错误		

3415	判断题	根据GB/T 39786《信息安全技术 信息系统密码应用基本要求》，在密码应用攻防对抗演习中发现的密码应用安全缺陷，由于不是在密评中发现的，所以不必进行整改。	正确	错误		
3416	判断题	根据GB/T 39786《信息安全技术 信息系统密码应用基本要求》，密钥管理对于保证密钥全生存周期的安全性是至关重要的，可以保证密钥（除公钥外）不被非授权的访问、使用、泄漏、修改和替换，可以保证公钥不被非授权的修改和替换。	正确	错误		
3417	判断题	根据GB/T 39786《信息安全技术 信息系统密码应用基本要求》，密钥备份行为是审计涉及的范围，有必要生成审计信息，包括备份的主体、备份的时间等。	正确	错误		
3418	判断题	根据GB/T 39786《信息安全技术 信息系统密码应用基本要求》，密钥生成是密钥生存周期的起点，所有密钥都应当直接或间接地根据随机数生成。	正确	错误		
3419	判断题	根据GB/T 39786《信息安全技术 信息系统密码应用基本要求》，当公钥证书到期后，对应的公钥和私钥仍然可以正常使用。	正确	错误		
3420	判断题	根据GB/T 39786《信息安全技术 信息系统密码应用基本要求》，密钥销毁和密钥撤销的含义相同，都是对密钥进行删除。	正确	错误		
3421	判断题	根据GB/T 39786《信息安全技术 信息系统密码应用基本要求》，并非所有密钥都需要存储，一些临时密钥或一次一密的密钥在使用完就要立即进行销毁。	正确	错误		

3422	判断题	根据GB/T 39786《信息安全技术 信息系统密码应用基本要求》，公钥可以以明文方式在密码产品外存储、传递和使用，但有必要采取安全防护措施，防止公钥被非授权篡改。	正确	错误		
3423	判断题	根据GB/T 39786《信息安全技术 信息系统密码应用基本要求》，把密钥存储在通用存储设备或系统（如数据库）中时，可以只利用杂凑密码算法对密钥进行完整性保护。	正确	错误		
3424	判断题	根据GB/T 39786《信息安全技术 信息系统密码应用基本要求》，为了保证密钥的安全性，密钥一般不能明文导出到密码产品外部。	正确	错误		
3425	判断题	根据GB/T 39786《信息安全技术 信息系统密码应用基本要求》，密钥分发既能通过人工（离线）方式进行，也可通过自动（在线）方式进行。	正确	错误		
3426	判断题	根据GB/T 39786《信息安全技术 信息系统密码应用基本要求》，签名密钥对的私钥不应进行归档。	正确	错误		
3427	判断题	根据GB/T 39786《信息安全技术 信息系统密码应用基本要求》，虽然不需要保护公钥的机密性，但在使用前（如签名验证或者密钥协商过程）需要验证公钥的完整性，以及实体与公钥的关联关系，以确保公钥来源的真实性。	正确	错误		
3428	判断题	根据GB/T 39786《信息安全技术 信息系统密码应用基本要求》，如果密钥生存周期管理由密码产品提供，那么无论密码产品是否具备商用密码产品认证证书，都能保证密钥的安全。	正确	错误		

3429	判断题	根据GB/T 39786《信息安全技术 信息系统密码应用基本要求》，密钥销毁过程是可逆的，需要时通过授权可以从销毁结果中恢复原密钥。	正确	错误		
3430	判断题	GB/T 39786《信息安全技术 信息系统密码应用基本要求》对密码应用第三级及以上信息系统，要求根据密码应用的实际情况,设置密钥管理员、密码安全审计员、密码操作员等关键安全岗位。	正确	错误		
3431	判断题	GB/T 39786《信息安全技术 信息系统密码应用基本要求》要求密码应用第四级信息系统的密钥管理员、密码安全审计员、密码操作员、密码设备开发者应由本机构的内部员工担任。	正确	错误		
3432	判断题	GB/T 39786《信息安全技术 信息系统密码应用基本要求》人员管理层面，要求密码应用第四级密码应用系统建立关键人员保密制度和调离制度,签订保密合同,承担保密义务。	正确	错误		
3433	判断题	GB/T 39786《信息安全技术 信息系统密码应用基本要求》对于密码应用所有等级的信息系统，在人员管理层面都要求包括定期进行安全岗位人员考核、建立关键人员保密制度和调离制度、建立密码应用岗位责任制度等。	正确	错误		
3434	判断题	GB/T 39786《信息安全技术 信息系统密码应用基本要求》对密码应用第四级信息系统在人员管理层面要求：密钥管理员、密码安全审计员、密码操作员应由本机构的内部员工或上级机构员工担任。	正确	错误		
3435	判断题	GB/T 39786《信息安全技术 信息系统密码应用基本要求》对密码应用第三级信息系统规定对关键岗位建立多人共管机制。	正确	错误		

3436	判断题	GB/T 39786《信息安全技术 信息系统密码应用基本要求》对密码应用第三级信息系统规定对关键岗位建立专人专管机制。	正确	错误		
3437	判断题	GB/T 39786《信息安全技术 信息系统密码应用基本要求》规定，密码应用第三级信息系统应定期对密码应用安全岗位人员进行考核。	正确	错误		
3438	判断题	根据GB/T 39786《信息安全技术 信息系统密码应用基本要求》，基于非对称密码的数字签名技术，可用于构建基于密码技术的身份鉴别协议。	正确	错误		
3439	判断题	根据GB/T 39786《信息安全技术 信息系统密码应用基本要求》，由于防火墙是一类网络安全产品，所以对于登录防火墙的管理员用户，不必使用基于密码技术的身份鉴别。	正确	错误		
3440	判断题	根据GB/T 39786《信息安全技术 信息系统密码应用基本要求》，如果使用基于AES、SHA-256和RSA-2048算法的SSL协议来实现远程管理通道安全，那么对远程管理通道安全进行风险评估时，存在高风险项。	正确	错误		
3441	判断题	根据GB/T 39786《信息安全技术 信息系统密码应用基本要求》，可以使用消息鉴别码（MAC）机制保证日志记录完整性。	正确	错误		
3442	判断题	根据GB/T 39786《信息安全技术 信息系统密码应用基本要求》，可以使用代码签名机制保证重要可执行程序完整性、重要可执行程序来源真实性。	正确	错误		

3443	判断题	根据GB/T 39786《信息安全技术 信息系统密码应用基本要求》，对于网络安全等级保护四级系统，如果设备的操作系统采用了强制访问控制机制，那么就需要考虑采用密码技术保证重要信息资源安全标记完整性。	正确	错误		
3444	判断题	根据GB/T 39786《信息安全技术 信息系统密码应用基本要求》，常用的银行U盾，是“智能密码钥匙”类密码产品。	正确	错误		
3445	判断题	根根据GB/T 39786《信息安全技术 信息系统密码应用基本要求》，据目前商用密码产品检测认证目录，“安全电子签章系统”是一类密码产品，但无需按照GB/T 37092或GM/T 0028来做密码模块安全分级。	正确	错误		
3446	判断题	根据GB/T 39786《信息安全技术 信息系统密码应用基本要求》，如果某一政务信息系统需采用电子认证服务，那么项目建设单位需选择具有电子政务电子认证服务资质的机构。	正确	错误		
3447	判断题	根据GB/T 39786《信息安全技术 信息系统密码应用基本要求》，如果某一政务信息系统采用电子认证服务的，那么项目建设单位只需选择在工商部门依法注册的电子认证服务机构。	正确	错误		
3448	判断题	根据GB/T 39786《信息安全技术 信息系统密码应用基本要求》，为特定行业、特定需求设计的专用算法及未公开的通用算法，在使用前可向密码主管部门咨询有关政策，获得同意后也可作为合规的密码算法使用。	正确	错误		

3449	判断题	GB/T 39786《信息安全技术 信息系统密码应用基本要求》中，网络和通信安全层面的“安全接入认证”是对从外部连接到内部网络的设备进行接入认证，确保接入网络的设备身份真实性。	正确	错误		
3450	判断题	GB/T 39786《信息安全技术 信息系统密码应用基本要求》对密码应用第四级信息系统提出了“安全接入认证”要求，宜采用密码技术对从外部连接到内部网络的设备进行接入认证，确保接入设备身份的真实性。	正确	错误		
3451	判断题	GB/T 39786《信息安全技术 信息系统密码应用基本要求》对密码应用第三级信息系统提出了“安全接入认证”要求，宜采用密码技术对从外部连接到内部网络的设备进行接入认证，确保接入设备身份的真实性。	正确	错误		
3452	判断题	GB/T 39786《信息安全技术 信息系统密码应用基本要求》规定，密码应用第三级信息系统采用的密码产品应达到GB/T37092二级及以上安全要求。	正确	错误		
3453	判断题	根据GB/T 39786《信息安全技术 信息系统密码应用基本要求》，在网络边界部署的IPSec VPN或SSL VPN设备，正确配置后，可以同时保证网络通信过程中数据的完整性和机密性。	正确	错误		
3454	判断题	GB/T 39786《信息安全技术 信息系统密码应用基本要求》中，网络和通信安全层面的身份鉴别与应用和数据安全层面的身份鉴别可以互相替代。	正确	错误		

3455	判断题	GB/T 39786《信息安全技术 信息系统密码应用基本要求》规定，密码应用第三级及以上信息系统应采用密码技术对通信实体进行身份鉴别，保证通信实体身份的真实性。	正确	错误		
3456	判断题	GB/T 39786《信息安全技术 信息系统密码应用基本要求》规定，密码应用第三级信息系统应采用密码技术对通信实体进行双向身份鉴别，保证通信实体身份的真实性。	正确	错误		
3457	判断题	GB/T 39786《信息安全技术 信息系统密码应用基本要求》规定，密码应用第三级信息系统应采用密码技术保证通信过程中重要数据的机密性。	正确	错误		
3458	判断题	GB/T 39786《信息安全技术信息系统密码应用基本要求》规定，在网络和通信安全层面“采用密码技术保证网络边界访问控制信息的完整性”，该要求只针对密码产品，防火墙的访问控制列表不在此范围内。	正确	错误		
3459	判断题	根据GB/T 39786《信息安全技术 信息系统密码应用基本要求》，电子门禁系统进出记录数据存储完整性可通过HMAC机制来实现。	正确	错误		
3460	判断题	根据GB/T 39786《信息安全技术 信息系统密码应用基本要求》，电子门禁记录数据存储完整性只能通过部署符合GM/T 0036《采用非接触卡的门禁系统密码应用技术指南》的电子门禁系统来实现。	正确	错误		
3461	判断题	GB/T 39786《信息安全技术 信息系统密码应用基本要求》规定，密码应用第三级信息系统物理和环境安全层面采用的密码产品宜达到GB/T 37092一级及以上要求。	正确	错误		

3462	判断题	GB/T 39786《信息安全技术 信息系统密码应用基本要求》中，物理和环境安全层面的身份鉴别要求是为了保证重要区域进入人员身份的真实性。	正确	错误		
3463	判断题	GB/T 39786《信息安全技术 信息系统密码应用基本要求》中，物理和环境安全层面中的重要区域通常指信息系统所在的物理机房。	正确	错误		
3464	判断题	根据GB/T 39786《信息安全技术 信息系统密码应用基本要求》，密码应用第三级的信息系统如果部署在云服务提供商的机房，物理和环境安全层面的要求就不再适用。	正确	错误		
3465	判断题	根据GB/T 39786《信息安全技术 信息系统密码应用基本要求》，视频监控记录数据存储完整性可通过CBC-MAC机制来实现。	正确	错误		
3466	判断题	根据GB/T 39786《信息安全技术 信息系统密码应用基本要求》，密码应用第二级信息系统应制定密码应用应急策略。	正确	错误		
3467	判断题	根据GB/T 39786《信息安全技术 信息系统密码应用基本要求》，密码应用第三级及以上信息系统，当密码应用安全事件发生时，应立即启动应急处置措施。	正确	错误		
3468	判断题	根据GB/T 39786《信息安全技术 信息系统密码应用基本要求》，对于密码应用第三级信息系统，当密码应用安全事件发生后，应及时向信息系统主管部门及归属的密码管理部门进行报告。	正确	错误		

3469	判断题	根据GB/T 39786《信息安全技术 信息系统密码应用基本要求》，对于密码应用第四级信息系统，当密码应用安全事件发生后，应及时向信息系统主管部门及归属的密码管理部门进行报告。	正确	错误		
3470	判断题	根据GB/T 39786《信息安全技术 信息系统密码应用基本要求》，对于密码应用第二级及以下信息系统，当密码应用安全事件发生后，不强制要求向信息系统主管部门或属地密码管理部门进行报告。	正确	错误		
3471	判断题	根据GB/T 39786《信息安全技术 信息系统密码应用基本要求》，对于密码应用第三级及以上信息系统，当密码应用安全事件处置完成后，应及时向信息系统主管部门和归属的密码管理部门报告事件发生情况及处置情况。	正确	错误		
3472	判断题	根据GB/T 39786《信息安全技术 信息系统密码应用基本要求》，对于所有密码应用等级的信息系统，都必须单独制定应急策略并定期演练。	正确	错误		
3473	判断题	根据GB/T 39786《信息安全技术 信息系统密码应用基本要求》，对于密码应用第三级信息系统，当密码应用安全事件发生后，如果处置得当、未发现损失，则不必向信息系统主管部门报告。	正确	错误		
3474	判断题	根据GB/T 39786《信息安全技术 信息系统密码应用基本要求》，对于密码应用第四级信息系统，当密码应用安全事件处置完成后，应越过属地密码管理部门，直接向国家密码管理部门报告。	正确	错误		

3475	判断题	根据GB/T 39786《信息安全技术 信息系统密码应用基本要求》，在密码应用第四级信息系统应用和数据安全层面，要求采用密码技术保证访问控制信息的完整性和机密性。	正确	错误		
3476	判断题	根据GB/T 39786《信息安全技术 信息系统密码应用基本要求》，在信息系统中，基于生物特征识别与匹配的身份鉴别，是一种基于密码技术的身份鉴别。	正确	错误		
3477	判断题	GB/T 39786《信息安全技术 信息系统密码应用基本要求》应用和数据安全层面的各个指标所涉及的密钥之间应相对独立，即使这些指标所提供的应用功能类似，但使用的密钥也不应相同。	正确	错误		
3478	判断题	根据GB/T 39786《信息安全技术 信息系统密码应用基本要求》，密码应用第三级信息系统应用和数据安全层面采用的密码产品宜达到GB/T 37092二级及以上要求。	正确	错误		
3479	判断题	根据GB/T 39786《信息安全技术 信息系统密码应用基本要求》，密码应用第四级信息系统应用和数据安全层面采用的密码产品宜达到GB/T 37092三级及以上要求。	正确	错误		
3480	判断题	根据GB/T 39786《信息安全技术 信息系统密码应用基本要求》，应用和数据安全的身份鉴别要求是为了保证登录信息系统的用户身份的真实性。	正确	错误		
3481	判断题	根据GB/T 39786《信息安全技术 信息系统密码应用基本要求》，密码应用第三级信息系统应采用密码技术保证信息系统应用的重要数据在传输过程中的完整性。	正确	错误		

3482	判断题	根据GB/T 39786《信息安全技术 信息系统密码应用基本要求》，密码应用第三级信息系统应采用密码技术保证信息系统应用的重要数据在存储过程中的完整性。	正确	错误		
3483	判断题	根据GB/T 39786《信息安全技术 信息系统密码应用基本要求》，密码应用第三级信息系统应采用密码技术保证信息系统应用的访问控制信息的完整性。	正确	错误		
3484	判断题	根据GB/T 39786《信息安全技术 信息系统密码应用基本要求》，应用和数据安全层面的身份鉴别措施，可以替代网络和通信安全层面的身份鉴别。	正确	错误		
3485	单项选择题	依据GM/T 0115《信息系统密码应用测评要求》，对于以下哪类条款，在排除掉“不适用”的前提下，允许由信息系统责任方自行决定是否按照相应测评指标要求进行测评和结果判定（）。	对于“可”的条款	对于“宜”的条款	对于“应”的条款	以上均正确
3486	单项选择题	依据GM/T 0115《信息系统密码应用测评要求》，对于以下哪类条款，在排除掉“不适用”的前提下，密评人员应根据信息系统的密码应用方案和方案评估意见决定其是否纳入标准符合性测评范围（）。	对于“可”的条款	对于“宜”的条款	对于“应”的条款	以上均正确
3487	单项选择题	依据GM/T 0115《信息系统密码应用测评要求》，经核实后发现，某信息系统确实不涉及某项测评指标对应的安全需求，那么这种情形对于以下哪类条款可视为“不适用”（）。	对于“可”的条款	对于“宜”的条款	对于“应”的条款	以上均正确

3488	单项选择题	依据GM/T 0115《信息系统密码应用测评要求》，以下说法正确的是（ ）。	在GM/T 0115《信息系统密码应用测评要求》中，通用测评要求对应的是第一级到第四级的密码应用要求	在GM/T 0115《信息系统密码应用测评要求》中，密码应用技术测评要求对应的是第一级到第四级的密码应用要求	在GM/T 0115《信息系统密码应用测评要求》中，密码应用管理测评要求对应的是第一级到第五级的密码应用要求	在GM/T 0115《信息系统密码应用测评要求》中，测评单元“密钥管理安全性”对应的是第一级到第四级的密码应用要求
3489	单项选择题	以下不属于GM/T 0115《信息系统密码应用测评要求》的内容是（ ）。	通用测评要求	整体测评要求	测评方案编制	测评结论
3490	单项选择题	根据GM/T 0115《信息系统密码应用测评要求》，以下不单独判定符合性的测评单元是（ ）。	密码产品合规性	安全接入认证	访问控制信息完整性	身份鉴别
3491	单项选择题	根据GM/T 0115《信息系统密码应用测评要求》，在对信息系统给出最终测评结论时，若判定为“基本符合”，则说明该系统的安全防护程度达到以下哪种情况（ ）。	未发现安全问题，不存在不符合和部分符合项	存在不符合和部分符合项，而且存在的安全问题会导致信息系统面临高等级安全风险	存在符合项和部分符合项，但存在的安全问题不会导致信息系统面临高等级安全风险，且综合得分不低于阈值	以上都不对
3492	单项选择题	依据GM/T 0115《信息系统密码应用测评要求》，某信息系统的网络和通信安全层面测评对象包括IPSec VPN通信信道和SSL VPN通信信道，密评人员经测评后发现，针对“通信数据完整性”测评单元，IPSec VPN通信信道符合要求，SSL VPN通信信道不符合要求。那么该信息系统在网络和通信安全层面“通信数据完整性”测评单元的最终判定结果为（ ）。	符合	部分符合	不符合	不适用

3493	单项选择题	依据GM/T 0115《信息系统密码应用测评要求》，在测评网络和通信安全层面时，如果通信过程采用SSL协议提供保护，经实际抓包后，通常查看握手协议的（ ）消息，来获取密码套件属性值，进而判定具体使用的密码算法。	Client Hello	Server Hello	Server Hello Done	Server Key Exchange
3494	单项选择题	依据GM/T 0115《信息系统密码应用测评要求》，在人员管理测评中发现，被测单位设置了密钥管理员、密码安全审计员、密码操作员岗位并定义岗位职责；并对关键岗位采用AB角机制，其中密钥管理员与密码安全审计员互为AB角，这种情况针对“建立密码应用岗位责任制度”测评指标最合适的判定结果是（ ）。	符合	部分符合	基本符合	不符合
3495	单项选择题	根据GM/T 0115《信息系统密码应用测评要求》，以下不属于管理制度层面测评实施内容的是（ ）。	核查是否定期对密码应用安全管理制度和操作规程的合理性和适用性进行论证和审定	核查是否对密码相关管理人员或操作人员的日常管理操作建立操作规程。	核查是否具有密码应用操作规程执行过程中留存的相关执行记录。	核查系统相关人员是否了解并遵守密码相关法律法规和密码应用安全管理制度。
3496	单项选择题	根据GM/T 0115《信息系统密码应用测评要求》，以下不是设备和计算安全层面的测评对象的是（ ）。	数据库管理系统	虚拟设备	OA办公系统	电子签章系统
3497	单项选择题	根据GM/T 0115《信息系统密码应用测评要求》，以下不是设备和计算安全层面第三级信息系统测评指标的是（ ）。	身份鉴别	远程管理通道安全	系统资源访问控制完整性	安全接入认证
3498	单项选择题	根据GM/T 0115《信息系统密码应用测评要求》，以下不属于建设运行层面第三级信息系统测评指标的是（ ）。	制定密码应用方案	制定密钥安全管理策略	投入运行前进行商用密码应用安全性评估	密钥管理规则

3499	单项选择题	根据GM/T 0115《信息系统密码应用测评要求》，在建设运行层面仅涉及第三级及以上信息系统测评指标的是（ ）。	制定密码应用方案	制定密钥安全管理策略	投入运行前进行商用密码应用安全性评估	定期开展密码应用安全性评估及攻防对抗演习
3500	单项选择题	根据GM/T 0115《信息系统密码应用测评要求》，以下不是建设运行层面第二级信息系统测评指标的是（ ）。	制定密码应用方案	制定密钥安全管理策略	投入运行前进行商用密码应用安全性评估，评估通过后系统方可正式运行	制定实施方案
3501	单项选择题	根据GM/T 0115《信息系统密码应用测评要求》，以下属于设备和计算安全层面测评内容的是（ ）。	登录SSL VPN时的身份鉴别方式	登录应用系统时的身份鉴别方式	应用系统的访问控制信息	互联网SSL VPN接入系统内网时建立的SSL通道
3502	单项选择题	根据GM/T 0115《信息系统密码应用测评要求》，以下属于设备和计算安全层面测评内容的是（ ）。	核查是否采用密码技术对设备操作人员等登录设备的用户进行身份鉴别	核查是否采用密码技术对网络边界访问控制信息进行完整性保护	核查是否采用密码技术对从外部连接到内部网络的设备进行接入认证	核查是否采用密码技术对应用的重要信息资源安全标记进行完整性保护
3503	单项选择题	依据GM/T 0115《信息系统密码应用测评要求》，以下不属于云平台在设备和计算安全层面的测评对象的是（ ）。	物理服务器	虚拟服务器	云上应用	云服务器密码机
3504	单项选择题	依据GM/T 0115《信息系统密码应用测评要求》，某信息系统在互联网通过SSL VPN接入内网后，再通过堡垒机集中管理服务器，则在设备和计算安全层面“远程管理通道安全”应测评的内容为（ ）。	管理员客户端与SSL VPN之间的通道	堡垒机与服务器之间的通道	管理员客户端与SSL VPN之间的通道、SSL VPN与堡垒机之间的通道	SSL VPN与堡垒机之间的通道、堡垒机与服务器之间的通道

3505	单项选择题	依据GM/T 0115《信息系统密码应用测评要求》，对于第二级信息系统，下列应急处置层面测评实施中正确的是（ ）。	核查被测单位是否根据密码产品提供的安全策略处置密码应用安全事件	核查是否根据密码应用安全事件等级制定了应急策略并对应急策略进行评审	如发生过密码应用安全事件，核查事件发生后是否向信息系统主管部门提交了安全事件报告	如发生过密码应用安全事件，核查事件处置完成后是否向信息系统主管部门提交了事件发生情况及处置情况报告
3506	单项选择题	依据GM/T 0115《信息系统密码应用测评要求》，应用和数据安全层面“身份鉴别”指标主要核查（ ）用户登录的身份鉴别机制。	数据库管理员	服务器管理员	应用管理员	所有登录应用进行操作的实体
3507	单项选择题	依据GM/T 0115《信息系统密码应用测评要求》，某OA办公系统面向被测单位办公人员提供在线办公、公文意见签批等服务，管理员登录后台进行系统管理操作。经测评，办公人员身份鉴别判定为“不符合”，管理员身份鉴别判定为“符合”，则针对应用和数据安全层面的“身份鉴别”测评单元，最终判定结果为（ ）。	符合	部分符合	不符合	无法判定
3508	单项选择题	依据GM/T 0115《信息系统密码应用测评要求》，下列关于应用和数据安全层面“重要数据传输完整性”测评实施的说法中，错误的是（ ）。	从密码算法、密码技术、密码产品、密码服务、密钥管理方面进行通用测评	利用协议分析工具，分析受完整性保护的数据在传输时的数据格式（如签名长度、MAC长度）是否符合预期	如果使用数字签名技术进行完整性保护，可使用私钥对抓取的签名结果进行验证	如果以外接服务器密码机等密码产品的形式实现，需要核实密码产品是否真正被调用

3509	单项选择题	依据GM/T 0115《信息系统密码应用测评要求》，在对应用和数据安全中的“重要数据存储完整性”指标测评时，采用以下（ ）密码技术无法被判定为符合。	采用SM3-HMAC算法计算消息鉴别码	仅采用SM3算法计算杂凑值	使用SM4-CBC模式生成消息鉴别码，其中初始向量为全0，消息长度为约定好的固定长度	使用SM3和SM2算法计算签名值
3510	单项选择题	按照GM/T 0115《信息系统密码应用测评要求》，以下（ ）不属于应用和数据安全层面的测评内容。	重要信息资源安全标记完整性	访问控制信息完整性	日志记录存储完整性	重要可执行程序完整性和来源真实性
3511	单项选择题	依据GM/T 0115《信息系统密码应用测评要求》，下列关于应用和数据安全层面“重要数据存储机密性”指标测评实施和结果判定的说法中错误的是（ ）。	如调用外部密码产品实现，可以通过核查密码产品日志记录或配置信息等来判断使用密码算法的合规性	存储机密性保护通过具有商用密码产品认证证书的服务器密码机实现，则该测评指标的测评结果一定为“符合”	密码运算和密钥管理均由服务器密码机等合规的密码产品实现，但密钥管理安全性不一定为“符合”	可直接读取存储的重要数据，以判断机密性保护措施是否有效
3512	单项选择题	依据GM/T 0115《信息系统密码应用测评要求》，对于应用和数据安全层面“重要数据存储完整性”测评，以下说法不正确的是（ ）。	可以核查应用系统是否采用基于公钥密码算法的数字签名机制等密码技术对重要数据进行存储过程中的完整性保护	可以核查应用系统是否采用基于对称密码算法或密码杂凑算法的消息鉴别码机制等密码技术对重要数据进行存储过程中的完整性保护	如果没有采用基于公钥密码算法的数字签名机制、基于对称密码算法或密码杂凑算法的消息鉴别码机制等密码技术，则不符合本单元测评指标要求	如果没有采用经商用密码认证机构认证合格的密码产品实现存储完整性保护，则不符合本单元测评指标要求
3513	单项选择题	根据GM/T 0115《信息系统密码应用测评要求》，以下哪项测评指标在密码应用技术测评要求的四个安全层面均有涉及（ ）。	重要数据传输机密性	身份鉴别	日志记录完整性	不可否认性

3514	单项选择题	依据GM/T 0115《信息系统密码应用测评要求》，对于“宜”的条款，以下做法不正确的是（）。	若纳入标准符合性测评范围，则密评人员应按照相应测评指标要求进行测评和结果判定	若未纳入标准符合性测评范围，密评人员不仅要按照相应测评指标要求进行测评和结果判定，还应在测评中进一步确认是否存在其他风险控制措施	若未纳入标准符合性测评范围，密评人员在测评中应进一步核实密码应用方案中所描述的风险控制措施使用条件在实际的信息系统中是否被满足，且信息系统的实施情况与所描述的风险控制措施是否一致	若未纳入标准符合性测评范围，经密评人员确认信息系统实际采用的风险控制措施使用条件和具体措施与密码应用方案保持一致，则相应测评指标视为“不适用”
3515	单项选择题	依据GM/T 0115《信息系统密码应用测评要求》，密评机构在对某行业信息系统测评过程中，发现系统中使用了某特殊算法（由经检测认证的密码产品实现），系统方出具了国家密码管理部门同意在该行业内使用该算法的证明文件，但该算法并未以国家标准或行业标准形式发布。针对此情形，“密码算法合规性”应选择以下哪种判定结果（）。	符合	部分符合	不符合	不适用
3516	单项选择题	依据GM/T 0115《信息系统密码应用测评要求》，密评机构在测评某信息系统时，发现移动端用户采用协同签名技术（由经检测认证的密码产品实现）完成应用系统的登录认证。但密评人员查阅密码相关标准后发现，该技术并未以密码相关国家标准或行业标准发布。针对此情形，“密码技术合规性”的判定较为合理的是（）。	部分符合	符合	不符合	不适用

3517	单项选择题	依据GM/T 0115《信息系统密码应用测评要求》，密评人员在测评某二级系统时，发现该系统在投入运行前有经过初次评估并编制了密码应用安全性评估报告，但整个系统的评估结论为“不符合”。那么“投入运行前进行密码应用安全性评估”测评单元的判定结果是（ ）。	符合	部分符合	不符合	不适用
3518	单项选择题	依据GM/T 0115《信息系统密码应用测评要求》，某信息系统涉及2个物理机房。根据密码应用方案和现场测评结果，其中1个物理机房的物理和环境安全层面“身份鉴别”项测评结果为不适用，另1个物理机房符合要求。那么，该系统物理和环境安全层面“身份鉴别”测评单元，最终判定结果为（ ）。	符合	部分符合	不符合	不适用
3519	单项选择题	依据GM/T 0115《信息系统密码应用测评要求》，密评人员在测评时，以下（ ）情况可视为密钥管理方式较为安全。	将密钥进行切分为不同长度的子密钥，子密钥进行拼接后得到原始密钥	用于验签的公钥未采取任何保护措施存储到数据库中	加密密钥使用SM4-ECB算法加密后存储在外部数据库中	用于重要数据存储机密性保护的密钥存储在服务器密码机中
3520	单项选择题	依据GM/T 0115《信息系统密码应用测评要求》，某电子门禁系统通过自身的软件模块使用SM3算法计算门禁记录数据的杂凑值，并保存到数据库中，从而实现电子门禁记录数据的完整性保护，这种情况可判定为（ ）。	符合	部分符合	不符合	不适用

3521	单项选择题	依据GM/T 0115《信息系统密码应用测评要求》，在测评“网络和通信安全层面”时，如果通信过程采用IPSec协议提供保护，经实际抓包后，测评人员通常查看IPSec协议中（ ）阶段的报文数据，来获取密码算法属性值，进而确定具体使用的密码算法并进行结果判定。	IKE	AH	ESP	以上均可
3522	单项选择题	依据GM/T 0115《信息系统密码应用测评要求》，对于访问控制信息完整性，以下属于设备和计算安全层面测评内容的是（ ）。	部署在网络边界的VPN中的访问控制列表	通用服务器操作系统的系统权限访问控制信息	边界防火墙的ACL列表	应用系统的用户权限列表
3523	单项选择题	依据GM/T 0115《信息系统密码应用测评要求》，在设备和计算安全层面，使用以下哪种算法进行日志记录完整性保护的判定结果为不符合（ ）。	HMAC-SHA-1	CMAC-SM4	SM3WithSM2	SM3
3524	单项选择题	依据GM/T 0115《信息系统密码应用测评要求》，某信息系统部署和使用了2台A厂商具有B型号商用密码产品认证证书的服务器密码机，3台C厂商具有D型号商用密码产品认证证书的服务器密码机，则在“设备和计算安全”层面选取测评对象时应（ ）。	以服务器密码机作为测评对象	将5台服务器密码机均列为测评对象	将具有同一商用密码产品认证证书的服务器密码机作为一个测评对象	服务器密码机不作为设备和计算安全层面的测评对象
3525	单项选择题	依据GM/T 0115《信息系统密码应用测评要求》，某信息系统管理员在互联网通过合规的SSL VPN接入系统内网，管理员使用合规的智能密码钥匙登录SSL VPN，并正确启用国密算法，数字证书由合规的CA机构颁发，则网络和通信安全层面的“身份鉴别”指标应判定为（ ）。	符合	部分符合	不符合	无法判定

3526	单项选择题	依据GM/T 0115《信息系统密码应用测评要求》，某信息系统基于GMSSL协议使用安全浏览器访问堡垒机，GMSSL协议使用了基于SM3WithSM2算法的数字证书，且数字证书由合规的CA机构颁发，则堡垒机的“身份鉴别”指标应判定为（ ）。	符合	部分符合	不符合	无法判定
3527	单项选择题	根据《商用密码应用安全性评估FAQ（第二版）》，某三级信息系统于2020年10月投入运行，于2021年10月进行首次密评，评估结论为基本符合，于2022年进行了第二次密评，则第二次密评时，“投入运行前进行密码应用安全性评估”应判定为（ ）。	符合	部分符合	不符合	不适用
3528	单项选择题	下列关于应用和数据安全层面“访问控制信息完整性”指标测评的说法中不正确的是（ ）。	被测应用系统无身份鉴别模块，则该项测评指标不适用	保护对象可能包括用户角色配置信息、角色权限配置信息	如使用数字签名技术进行完整性保护，则可使用公钥对存储的签名结果进行验证	如果以外接服务器密码机等密码产品的形式实现，还需要核实密码产品是否真正被调用
3529	单项选择题	依据GM/T 0115《信息系统密码应用测评要求》，某机关政务应用系统用户登录调用外部系统提供的身份鉴别服务，外部系统采用静态口令和手机验证码组合的身份鉴别方式，在对该政务应用系统进行应用和数据安全层面“身份鉴别”指标测评时，最合适的判定结果为（ ）。	符合	部分符合	不符合	不适用

3530	单项选择题	依据GM/T 0115《信息系统密码应用测评要求》，某网上银行系统在应用和数据安全层面“不可否认性”指标测评的具体对象包括用户关键交易操作、与外部系统的关键交易操作，经核查发现，关键交易操作不可否认性实现均采用数字签名技术，且密码产品、密码服务符合GM/T 0115通用测评要求，但部分网银用户仍使用RSA1024数字证书，则本单元的测评结果最合适的是（ ）。	符合	部分符合	不符合	无法判定
3531	单项选择题	依据GM/T 0115《信息系统密码应用测评要求》，现场测评环节，在对应用系统鉴别数据进行应用和数据安全层面“重要数据传输机密性”指标测评时，应用系统采取下列哪项技术措施可判定该测评对象机密性保护措施无效（ ）。	客户端对口令明文进行SHA-256杂凑运算后，将杂凑值传输至后台应用系统，应用系统对杂凑值进行比对	客户端调用智能密码钥匙，采用SM4算法对口令信息加密后传输	客户端采用服务端RSA-2048公钥对口令信息加密后传输	客户端采用AES算法对口令信息加密后传输
3532	单项选择题	依据GM/T 0115《信息系统密码应用测评要求》，被测应用系统面向业务用户提供WEB端和APP端2种访问方式，用户通过WEB端注册后，可使用相同账户名口令登录APP；当用户使用WEB浏览器登录应用系统时，通过智能密码钥匙对口令信息进行SM4加密后传输；用户登录手机端APP时，口令明文传输。则在进行应用和数据安全层面“重要数据传输机密性”测评时，口令信息测评结果为（ ）。	符合	部分符合	不符合	无法判定

3533	单项选择题	依据GM/T 0115《信息系统密码应用测评要求》，密评人员在对SSL VPN通信信道进行测评时，发现协议算法套件为TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA (0xc013)，以下判断合理的是（）。	采用ECDHE算法进行密钥协商	采用RSA算法来保证通信过程中数据的机密性	采用AES算法来保证通信过程中数据的完整性	采用SHA算法来保证通信过程中数据的完整性
3534	单项选择题	依据GM/T 0115《信息系统密码应用测评要求》，下列密码防护措施一定“不符合”应用和数据安全层面“重要数据传输机密性”测评指标要求的是（）。	采用SM4-CTR算法对重要用户信息加密后传输	采用SM2公钥加密算法对口令信息加密后传输	采用ZUC-EIA算法对重要用户信息加密后传输	采用ChaCha20-Poly1305算法对重要用户信息加密后传输
3535	单项选择题	根据GM/T 0115《信息系统密码应用测评要求》，关于整体测评要求的描述错误的是（ ）。	整体测评是在单元测评结束后执行的环节	存在“等效弥补”	整体测评环节可能涉及测评单元的分数调整	可能涉及单元间、层面间弥补的情形
3536	单项选择题	在测评某信息系统机房时，发现该机房有A和B两个门，其中机房管理员、设备维护和管理等人员通常从A门（使用经检测认证的电子门禁系统）刷门禁卡进入；B门（刷Mifare门禁卡进入）平时几乎不用。按照GM/T 0115《信息系统密码应用测评要求》，物理和环境安全层面“身份鉴别”指标的判定结果，最合适的是（ ）。	符合	部分符合	不符合	不适用

3537	单项选择题	某四级信息系统针对“电子门禁记录数据存储完整性”指标要求采取的措施为：门禁日志记录存储在日志审计系统（内置PCI-E密码卡）中，针对日志记录表单会生成一个MAC值（由HMAC-SHA256实现），日志审计系统将日志记录及对应MAC值保存至后台数据库（数据库登录方式为“用户名+口令”）。经密评人员核实，相关密码运算由密码卡完成，密码卡经检测认证合格。那么，依据GM/T 0115《信息系统密码应用测评要求》，针对该测评单元的判定结果较为合理的是（ ）。	符合	部分符合	不适用	不符合
3538	单项选择题	某等保三级信息系统，设备运维人员从互联网先访问网络边界设备SSL VPN网关（网络通道采用国密SSL协议保证安全性），再通过SSL VPN登录堡垒机，进而通过堡垒机完成对应用服务器的访问，堡垒机的“身份鉴别”判定结果为“符合”，应用服务器的登录方式为“用户名+口令”。针对此情形，应用服务器“身份鉴别”的判定结果为（）。	不符合	部分符合	符合	基本符合
3539	单项选择题	某云平台和云上应用系统的业务数据存储机密性保护，由同一台云服务器密码机（经检测认证）提供，且均采用SM4-CBC算法计算数据密文。若云平台率先通过密评，且“重要数据存储机密性”测评单元得到“符合”结论，那么依据GM/T 0115《信息系统密码应用测评要求》，云上应用系统的该测评指标应选择以下哪种判定结果更合适（）。	符合	部分符合	不符合	不确定，需重新测评

3540	单项选择题	某网上银行信息系统，网银用户持有银行配发的智能密码钥匙，在交易时，用户使用智能密码钥匙对交易信息进行SM9数字签名，网银服务端收到后调用签名验签服务器完成验签。上述密码运算均在密码产品中完成，密码产品均经过检测认证。依据GM/T 0115《信息系统密码应用测评要求》，则“不可否认性”最合适的判定结果是（ ）。	符合	部分符合	不符合	不确定
3541	单项选择题	依据GM/T 0115《信息系统密码应用测评要求》，某系统管理员使用智能密码钥匙登录服务器密码机进行身份鉴别，以下哪项不属于设备和计算安全层面应核查的内容（ ）。	服务器密码机的商用密码产品认证证书	智能密码钥匙的密码模块安全等级	利用协议分析工具，抓取应用系统调用密码机的指令报文，验证其是否符合预期	密码机设备日志记录
3542	单项选择题	依据GM/T 0115《信息系统密码应用测评要求》，某信息系统基于国密SSL协议使用安全浏览器访问堡垒机，国密SSL协议使用了基于SM3WithSM2算法的数字证书，则以下说法正确的是（ ）。	堡垒机“身份鉴别”测评项可判定为符合	数字证书签名算法OID为1.2.156.10197.1.501	测评人员可通过数字证书获取颁发者的公钥信息	数字证书签名算法OID为1.2.156.10197.1.502
3543	单项选择题	根据《商用密码应用安全性评估FAQ（第二版）》，对于建设运行层面的“投入运行前进行密码应用安全性评估”测评项，在2020年1月1日之后投入运行的系统，投入运行后进行首次密评时，该项判定为（ ）；如果是非首次密评，且前次密评结果为基本符合，该项可判定（ ）。	不符合、符合	不适用、符合	不符合、部分符合	部分符合、部分符合

3544	单项选择题	依据GM/T 0115《信息系统密码应用测评要求》，某信息系统使用了服务器密码机、签名验签服务器等密码产品，密码产品合规性核查要点不包含以下哪项内容（ ）。	核查密码产品是否具备商用密码产品认证证书	核查服务器密码机的随机数发生器是否采用国家密码管理主管部门批准的物理噪声源芯片	若密码产品符合密码模块相关标准，则核查其密码模块是否达到相应安全等级要求	核查商用密码产品认证证书是否在有效期内
3545	单项选择题	密评人员在测评时发现被测系统调用服务器密码机，对堡垒机的访问控制信息进行完整性保护，并获取了堡垒机访问控制信息的完整性校验值为：0x1073f2a58ae7e43550bc1c11f4cd2899，其长度为128比特，以下说法错误的是（ ）。	一定未采用HMAC-SM3算法对堡垒机访问控制信息进行完整性保护	可能采用了HMAC-SM3算法对堡垒机访问控制信息进行完整性保护	可能采用了HMAC-MD5算法对堡垒机访问控制信息进行完整性保护	可能采用了基于SM4-CBC的MAC算法对堡垒机访问控制信息进行完整性保护
3546	单项选择题	依据GM/T 0115《信息系统密码应用测评要求》，在对三级信息系统开展设备和计算安全层面的密评时，以下身份鉴别方式符合密评要求的是（ ）。	该系统设置3名设备管理员，并为每名管理员配备了合规的智能密码钥匙和相同的数字证书，并使用合规的密码技术实现了管理员登录的身份鉴别	系统管理员使用合规的智能密码钥匙登录SSL VPN时，SSL VPN仅比对智能密码钥匙发送的唯一标识符	使用合规的动态令牌登录堡垒机，服务端部署合规的动态令牌认证系统，并正确启用国密算法	使用合规的智能密码钥匙登录堡垒机，智能密码钥匙的PIN码为6位数字，错误口令登录次数限制为12次

3547	单项选择题	依据GM/T 0115《信息系统密码应用测评要求》，关于设备和计算安全层面的密评，以下说法正确的是（ ）。	若某信息系统技术人员通过自研软件使用HMAC-SM3算法对堡垒机访问控制信息进行完整性保护，则堡垒机的访问控制信息完整性一项可判定为符合	某四级信息系统，使用的服务器密码机（安全等级二级）具有合格的商用密码产品认证证书，且可以确定实际部署的密码产品与获认证产品一致，考虑到密码产品功能确定且自身安全防护能力较高，针对该密码机在设备和计算安全层面的“系统资源访问控制信息完整性”“日志记录完整性”“重要可执行程序完整性、重要可执行程序来源真实性”这三个指标，均可直接判定为“符合”	当堡垒机的管理员有多种身份鉴别方式时，应对不同的身份鉴别方式分别进行测评，并以最低分作为量化评估的结果。	依照GM/T 0115《信息系统密码应用测评要求》，设备和计算安全层面“身份鉴别”测评指标“采用密码技术对登录设备的用户进行身份鉴别”中，要求的用户指的是登录设备的用户，同时也指登录设备中应用系统的用户
3548	单项选择题	依据GM/T 0115《信息系统密码应用测评要求》，应用系统采用数字签名技术实现用户身份鉴别，经核实签名算法标识，可认为密码算法符合通用测评要求的是（）。	1.2.156.10197.1.301	1.2.840.10045.2.1	1.2.840.10045.5.1	1.2.156.10197.1.501

3549	单项选择题	依据GM/T 0115《信息系统密码应用测评要求》，某信息系统部署经商用密码产品认证机构认证合格的SSL安全网关代理业务应用系统进行基于SM2数字签名技术的用户身份鉴别，用户经SSL安全网关鉴别通过后，再采用静态口令登录应用系统；在数字签名身份鉴别机制通用测评要求判定为“符合”的前提下，应用和数据安全层面“身份鉴别”指标最可能的判定结果为（ ）。	符合	部分符合	不符合	无法判定
3550	单项选择题	依据GM/T 0115《信息系统密码应用测评要求》，在对应用和数据安全层面中的“身份鉴别”指标测评时，获取下列哪项测评证据的判定结果一定为“不符合”（ ）。	WEB端业务用户采用智能密码钥匙登录应用系统	WEB端业务用户使用手机APP客户端扫码登录业务应用系统，手机APP集成手机盾SDK，服务端调用了协同签名平台进行签名验证	移动端用户可采用SM2协同签名技术登录手机APP（集成移动终端密码模块SDK）。	系统管理员采用短信验证码登录业务应用系统，服务端动态口令认证模块基于开源代码实现
3551	单项选择题	依据GM/T 0115《信息系统密码应用测评要求》，某应用系统面向业务用户提供WEB端和APP端2种访问方式，在WEB端，用户浏览器与应用系统服务端采用国密SSL协议（国密浏览器实现）保障通信数据机密性，APP客户端与应用系统服务端之间采用HTTP协议传输，经核查发现应用系统用户鉴别数据均以明文方式传输，经整体测评后，鉴别数据在应用和数据安全层面“重要数据传输机密性”指标的测评结果最可能为（ ）。	符合	部分符合	不符合	无法判定

3552	单项选择题	在对应用和数据安全层面中的“重要数据存储机密性”指标测评时，采用以下（ ）密码技术可能被判定为“部分符合”。	采用SM3算法对业务数据计算杂凑值后存储	采用DES算法对重要业务数据加密后存储	采用SM4-ECB模式对所有用户性别信息项进行加密后存储	使用RSA算法对个人敏感信息加密后存储
3553	单项选择题	应用和数据安全层面测评时，发现被测应用系统采用SM3算法对口令计算杂凑值后传输和存储，且客户端调用了经商用密码认证机构认证合格的智能密码钥匙生成MAC，则“身份鉴别”指标判定结果为（ ）。	符合	部分符合	不符合	无法判定
3554	单项选择题	依据GM/T 0115《信息系统密码应用测评要求》，在针对网络和通信安全层面的“身份鉴别”指标进行测评时，SSL协议工作流程中，如果服务端需要验证客户端的身份，则测评人员需要核查服务端需向客户端发送的（ ）消息。	Server Key Exchange	Certificate Request	Server Certificate	Certificate Verify
3555	单项选择题	依据GM/T 0115《信息系统密码应用测评要求》，密评人员在对某三级信息系统测评时，发现“应用和数据安全”层面的重要数据传输完整性采用签名验签服务器（经检测认证合格，安全等级二级）提供保护。签名验签服务器采用“口令+智能IC卡”的方式鉴别设备管理员，但设备管理员将智能IC卡长期插入签名验签服务器使用。针对此情形，关于“密码产品合规性”的判定较为合理的是（ ）。	符合	部分符合	不符合	不适用

3556	单项选择题	依据GM/T 0115《信息系统密码应用测评要求》，对某信息系统进行“网络和通信安全”层面测评时发现，该系统客户端与服务端通信报文采用SM4算法进行加密后传输，算法为开发人员自己实现（算法实现未经正确性验证），加密密钥嵌入在代码中且不可更改。因此，“通信过程中重要数据的机密性”测评指标最合适的判定结果是（）。	符合	部分符合	不符合	不适用
3557	单项选择题	某信息系统管理员使用合规的智能密码钥匙登录服务器密码机时，若服务器密码机仅通过比对智能密码钥匙发送的唯一标识符进行鉴别，则身份鉴别测评项的判定结果为（ ）。	符合	部分符合	不符合	无法判定
3558	单项选择题	在对应急处置层面“应急策略”指标测评时发现，某第三级信息系统制定了符合网络安全等级保护基本要求的应急预案，预案中明确了网络安全事件发生时的应急处理流程、系统恢复流程及其他管理措施，具有事件处置记录模板，但应急预案未涵盖密码应用安全相关事件且信息系统尚未发生密码应用安全事件。依据GM/T 0115《信息系统密码应用测评要求》,本指标判定结果最合适的是（ ）。	符合	部分符合	不符合	无法判定

3559	单项选择题	某已建信息系统依据GM/T 39786第三级要求进行密码应用改造过程中，制定并正式发布了密码应用安全管理制度，制度中包含应急处置相关规定，其中要求密码应用安全事件处置完成后应及时向信息系统主管部门及归属的密码管理部门报告事件发生情况及处置情况，并制定了应急处置记录模板及安全事件报告模板；信息系统自投入运行以来尚未发生密码应用安全事件；经核查该系统密码应用方案及其评估意见，管理指标均为适用。则密评机构在开展应急处置层面“向有关主管部门上报处置情况”指标测评时，依据GM/T 0115《信息系统密码应用测评要求》，最合适的判定结果为（　）。	符合	部分符合	不符合	不适用
3560	多项选择题	GM/T 0115《信息系统密码应用测评要求》中定义的测评单元包括以下哪些要素（）。	测评指标	测评对象	测评实施	结果判定
3561	多项选择题	GM/T 0115《信息系统密码应用测评要求》适用于指导信息系统哪些环节的密码应用安全性评估工作（）。	规划	建设	运行	运维
3562	多项选择题	对第五级密码应用测评要求的描述，在GM/T 0115《信息系统密码应用测评要求》中哪些部分有出现（）。	安全接入认证	身份鉴别	密码技术合规性	密钥管理安全性
3563	多项选择题	GM/T 0115《信息系统密码应用测评要求》包含了以下哪些内容（）。	通用测评要求	整体测评要求	风险分析和评价	密码可用性测评要求
3564	多项选择题	GM/T 0115《信息系统密码应用测评要求》中，术语“核查”包括了哪些实际测评时的测评方式（）。	访谈	文档审查	配置检查	工具测试

3565	多项选择题	根据GM/T 0115《信息系统密码应用测评要求》，下列说法正确的是（）。	单元测评可以和整体测评同时执行	每个安全层面的单元测评理论上可以同时执行	风险分析和评价是在单元测评和整体测评完成后执行的	测评结论主要由整体测评后的分数得到，风险分析和评价不影响测评结论，只是附加说明系统中的安全问题对应的安全风险程度高低
3566	多项选择题	对于二级信息系统，以下哪些测评指标可由信息系统责任方自行决定是否按照GM/T 0115《信息系统密码应用测评要求》中该测评指标要求进行测评和结果判定（　　）。	身份鉴别	电子门禁记录数据存储完整性	通信数据完整性	日志记录完整性
3567	多项选择题	GM/T 0115《信息系统密码应用测评要求》中，不单独判定符合性的测评单元有以下哪些（）。	密码算法合规性	密码产品合规性	身份鉴别	密钥管理有效性
3568	多项选择题	以下属于GM/T 0115《信息系统密码应用测评要求》中通用测评要求内容的是（）。	密码算法合规性	密码技术合规性	密码产品合规性	密钥管理安全性
3569	多项选择题	依据GM/T 0115《信息系统密码应用测评要求》，以下选项中属于设备和计算安全层面测评对象的有（）。	应用服务器	虚拟机	数据库	金融数据密码机
3570	多项选择题	依据GM/T 0115《信息系统密码应用测评要求》，信息系统的应用用户可能包含以下哪些（）。	互联网用户	单位内部用户	应用服务器设备管理员	应用管理员
3571	多项选择题	根据GM/T 0115《信息系统密码应用测评要求》，关于应用和数据安全层面“不可否认性”测评单元，以下描述正确的是（）。	该测评指标通常针对于三级和四级信息系统	通常可采用基于公钥密码算法的数字签名机制实现该密码功能	核查内容包含数据原发行为的不可否认性	核查内容包含数据存储行为的不可否认性
3572	多项选择题	根据GM/T 0115《信息系统密码应用测评要求》，一个信息系统的测评结论可以是以下哪些（）。	符合	基本符合	不符合	部分符合

3573	多项选择题	GM/T 0115《信息系统密码应用测评要求》的资料性附录包括以下哪些（）。	密钥生存周期管理检查要点	典型密码产品应用测评技术	典型密码产品管理测评技术	典型密码功能测评技术
3574	多项选择题	根据GM/T 0115《信息系统密码应用测评要求》，以下结果判定方法正确的是（）。	针对单个测评对象，如果某测评单元的测评实施内容均为是，则该测评对象符合这个测评单元的测评指标要求。	针对单个测评对象，如果某测评单元的测评实施内容均为否，则该测评对象不符合本单元的测评指标要求。	针对某个测评单元，对该单元涉及的所有测评对象的判定结果进行汇总，如果判定结果均为符合，则本单元的测评结果为符合。	针对某个测评单元，对该单元涉及的所有测评对象的判定结果进行汇总，如果判定结果均为不符合，则本单元的测评结果为不符合。
3575	多项选择题	根据GM/T 0115《信息系统密码应用测评要求》，采用下列哪些鉴别技术，物理机房电子门禁系统的“身份鉴别”指标可以判定为“符合”（）。	动态口令	基于对称密码算法或密码杂凑算法的消息鉴别码（MAC）机制	基于公钥密码算法的数字签名机制	指纹识别
3576	多项选择题	根据GM/T 0115《信息系统密码应用测评要求》，以下哪些选项属于物理和环境安全层面在测评时应该关注的对象（）。	信息系统所在机房等重要区域	信息系统所在机房等重要区域的电子门禁系统	信息系统所在机房等重要区域的视频监控系统	信息系统所在机房等重要区域部署的防病毒系统
3577	多项选择题	根据GM/T 0115《信息系统密码应用测评要求》，对于三级信息系统，物理和环境安全的测评关注点包括信息系统所在机房等重要区域及其（）。	动力环境监控系统	电子门禁系统	消防联动控制系统	视频监控系统
3578	多项选择题	根据GM/T 0115《信息系统密码应用测评要求》，在对物理和环境安全层面“视频监控记录数据存储完整性”指标进行测评时，应核查是否采用（）等密码技术对视频监控音像记录数据进行存储完整性保护，并验证完整性保护机制是否正确和有效。	基于对称算法的加解密机制	基于对称算法的消息鉴别码机制	基于密码杂凑算法的消息鉴别码机制	基于公钥密码算法的数字签名机制

3579	多项选择题	根据GM/T 0115《信息系统密码应用测评要求》，以下哪些选项属于网络和通信安全层面的测评关注点（ ）。	信息系统与网络边界外建立的网络通信息信道	提供网络通信保护功能的设备、组件、密码产品	信息系统中互联网接入区的入侵检测系统	提供入网接入认证功能的设备或组件、密码产品
3580	多项选择题	根据GM/T 0115《信息系统密码应用测评要求》，下列关于网络和通信安全层面“身份鉴别”测评指标的测评过程描述哪些是正确的（ ）。	通过访谈，了解采用了哪种通信实体身份鉴别实现机制	核查并验证身份鉴别机制是否正确有效	核查采用的密码算法和密码技术是否合规	核查采用的密钥管理措施是否安全
3581	多项选择题	根据GM/T 0115《信息系统密码应用测评要求》，下面哪些属于管理制度方面测评的对象（ ）。	密钥管理制度及策略类文档	密码人员管理制度	服务器密码机操作规程	管理制度修订记录
3582	多项选择题	根据GM/T 0115《信息系统密码应用测评要求》，下列哪些属于对密码相关管理人员或操作人员的日常管理操作建立的操作规程（ ）。	服务器密码机配置流程	门禁卡发卡操作规程	密钥管理系统操作规程	年度人员培训计划
3583	多项选择题	根据GM/T 0115《信息系统密码应用测评要求》，核查关键岗位人员的保密协议时，应核查协议中是否包括下列哪些内容（ ）。	保密范围	保密责任和违约责任	协议的有效期限	责任人的签字
3584	多项选择题	根据GM/T 0115《信息系统密码应用测评要求》，在进行“建立上岗人员培训制度”指标的测评时，下列哪些在其测评对象范围内（ ）。	安全主管	密钥管理员	密码安全审计员	密码操作员
3585	多项选择题	根据GM/T 0115《信息系统密码应用测评要求》，密评人员在对某信息系统进行密评时，判定密码产品合规性时应从以下哪些方面实施测评（ ）。	了解信息系统中密码产品的型号和版本等配置信息	核查密码产品是否经商用密码认证机构认证合格	核查密码产品的使用是否满足其安全运行的条件，如其安全策略或使用手册说明的部署条件	依据密码模块相关标准的密码产品，还要核查密码产品是否满足密码模块相应安全等级及以上安全要求
3586	多项选择题	依据GM/T 0115《信息系统密码应用测评要求》，在实施信息系统“密钥管理安全性”测评时，除核查密钥管理安全性实现技术是否正确有效外，还应核查密钥管理使用的（ ）是否满足要求。	密码算法	密码技术	密码产品	密码服务

3587	多项选择题	依据GM/T 0115《信息系统密码应用测评要求》，在测评信息系统“具备密码应用安全管理制度”指标时，密评人员应核查各项安全管理制度包括（）等制度。	密码人员管理	密钥管理	应急处置	密码软硬件及介质管理
3588	多项选择题	根据GM/T 0115《信息系统密码应用测评要求》，密评人员在对“密钥管理规则”指标进行测评时，应核查（）。	是否有通过评估的密码应用方案	是否根据密码应用方案建立相应密钥管理规则	是否对密钥管理规则进行评审	信息系统中密钥是否按照密钥管理规则进行生存周期的管理
3589	多项选择题	某信息系统部署于两个自建机房，机房之间通过光纤连接，启用防火墙的IPSec VPN对机房之间的业务流量进行保护，通过服务器密码机对应用服务器的日志记录进行完整性保护。根据GM/T 0115《信息系统密码应用测评要求》，以下作为设备和计算安全层面测评对象的是（）。	应用服务器	服务器密码机	光纤连接器	防火墙
3590	多项选择题	根据GM/T 0115《信息系统密码应用测评要求》，以下可作为设备和计算安全层面测评对象的是（）。	具有密码功能的网络及安全设备	服务器密码机	密钥管理系统	数据库管理系统
3591	多项选择题	根据GM/T 0115《信息系统密码应用测评要求》，设备和计算安全层面，系统资源访问控制信息主要包括（　）。	操作系统文件目录的访问控制信息	设备操作系统的系统权限访问控制信息	堡垒机等第三方运维系统中的权限访问控制信息	数据库中的数据访问控制信息

3592	多项选择题	根据GM/T 0115《信息系统密码应用测评要求》，在设备和计算安全层面，以下属于“身份鉴别”指标的测评实施内容的是（ ）。	核查身份鉴别所使用的密码算法合规性、密钥技术合规性	核查身份鉴别所使用的密码产品合规性、密码服务合规性，以及相关密钥管理安全性	核查是否采用动态口令机制、基于对称密码算法或密码杂凑算法的消息鉴别码、基于公钥密码算法的数字签名机制等密码技术对设备操作人员等登录设备的用户进行身份鉴别	验证登录设备的用户身份真实性实现机制是否正确和有效
3593	多项选择题	依据GM/T 0115《信息系统密码应用测评要求》，能够确认密码产品具有合格的商用密码产品认证证书，且可以确定实际部署的密码产品与获认证产品一致的情况下，针对整机类密码产品，在设备和计算安全层面，以下哪些指标项可判定为符合（ ）。	系统资源访问控制信息完整性	日志记录完整性	身份鉴别	重要可执行程序完整性、重要可执行程序来源真实性
3594	多项选择题	根据GM/T 0115《信息系统密码应用测评要求》，以下属于二级信息系统“设备和计算安全”层面测评项的是（ ）。	身份鉴别	远程管理通道安全	系统资源访问控制信息完整性	日志记录完整性
3595	多项选择题	根据GM/T 0115《信息系统密码应用测评要求》，以下属于三级信息系统“建设运行”方面测评项的是（ ）。	制定密码应用方案	定期开展密码应用安全性评估及攻防对抗演习	制度执行过程记录留存	建立操作规程
3596	多项选择题	根据GM/T 0115《信息系统密码应用测评要求》，以下属于“定期开展密码应用安全性评估及攻防对抗演习”测评实施要点的是（ ）。	核查信息系统投入后，是否定期开展密码密码应用安全性评估及攻防对抗演习	核查密码应用安全事件发生后，是否及时向信息系统主管部门进行报告	核查是否根据密码应用安全事件等级制定了相应的密码应用应急策略并对应急策略进行评审	核查信息系统投入后，是否具有密码应用安全性评估报告及攻防对抗演习报告

3597	多项选择题	根据GM/T 0115《信息系统密码应用测评要求》，以下属于密钥分发检查要点的是（）。	确认系统内部采用何种密钥分发方式	确认密钥备份的审计信息是否包括备份的主体、时间等信息	确认信息系统内部是否具有密钥的更新策略	确认密钥传递过程中信息系统使用了哪些密码技术对密钥进行处理以保护其机密性、完整性与真实性，并核实保护措施使用的正确性和有效性
3598	多项选择题	根据GM/T 0115《信息系统密码应用测评要求》，关于设备和计算安全层面“日志记录完整性”测评指标，以下属于该项密钥管理核查内容的是（）。	若密钥管理使用的密码产品符合密码模块相关标准，则核查相关密码产品是否满足密码模块相应安全等级及以上安全要求	核查密钥管理安全性实现技术是否正确有效	核查日志记录是否进行备份以及备份机制是否合理	核查相关密码产品是否按照产品配套的安全策略文档进行部署和使用
3599	多项选择题	根据GM/T 0115《信息系统密码应用测评要求》，以下属于三级信息系统“设备和计算安全”层面测评指标的是（）。	安全接入认证	远程管理通道安全	重要信息资源安全标记完整性	日志记录完整性
3600	多项选择题	依据GM/T 0115《信息系统密码应用测评要求》，信息系统应用的重要数据包括但不限于（）。	鉴别数据	访问控制信息	重要业务数据	个人敏感信息
3601	多项选择题	依据GM/T 0115《信息系统密码应用测评要求》，应用和数据安全层面的完整性保护对象有（）。	安全标记	访问控制信息	需要传输的重要数据	需要存储的重要数据
3602	多项选择题	依据GM/T 0115《信息系统密码应用测评要求》，以下哪些指标不属于应用和数据安全层面的测评指标（ ）。	身份鉴别	系统资源访问控制信息完整性	重要信息资源安全标记完整性	重要可执行程序完整性、重要可执行程序来源真实性

3603	多项选择题	被测业务应用在身份鉴别、重要数据传输机密性、重要数据传输完整性方面均未采用密码技术，整体测评时，依据GM/T 0115《信息系统密码应用测评要求》，下列哪些测评指标的测评结果可能会对应用和数据安全层面进行弥补（）。	网络和通信安全层面“身份鉴别”	网络和通信安全层面“通信过程中重要数据的机密性”	网络和通信安全层面“通信数据完整性”	设备和计算安全层面“身份鉴别”
3604	多项选择题	依据GM/T 0115《信息系统密码应用测评要求》，下列可能作为应用和数据安全层面“重要数据存储机密性”测评指标具体测评对象的是（）。	鉴别数据	身份证号	重要业务数据	重要信息资源安全标记
3605	多项选择题	根据GM/T 0115《信息系统密码应用测评要求》附录C提供的测评技术，在对三级信息系统进行应用和数据安全层面“重要数据存储完整性”指标测评时，预期结果包括（）。	数据格式（签名长度、MAC长度）符合预期	若调用外接密码产品实现，则调用指令、次数等符合预期	登录密码产品查看相关配置和密码功能调用日志，密钥配置、日志记录均显示使用合规的密码算法	篡改存储数据后，能够检测出存储数据的完整性受到了破坏
3606	多项选择题	依据GM/T 0115《信息系统密码应用测评要求》，下列可能作为应用和数据安全层面“重要数据存储完整性”测评指标具体测评对象的是（）。	鉴别数据	访问控制信息	重要业务数据	用户操作日志
3607	多项选择题	依据GM/T 0115《信息系统密码应用测评要求》，应急处置层面的测评对象包括（）。	密码应用应急策略	应急处置记录	攻防对抗演练记录	安全事件报告
3608	多项选择题	按照GM/T 0115《信息系统密码应用测评要求》中对测评对象的阐述，以下内容正确的是（）。	物理和环境安全层面的测评对象仅涉及电子门禁系统	网络和通信安全层面的测评对象包括内网环境中的设备远程运维通道	数据库及其管理系统属于设备和计算安全层面的测评对象	应用和数据安全层面的身份鉴别指标的测评对象是登录应用系统的用户
3609	多项选择题	以下属于GM/T 0115《信息系统密码应用测评要求》中通用测评要求内容的是（）。	密码算法合规性	密码产品正确性	密码服务合规性	密钥管理有效性

3610	多项选择题	在GM/T 0115《信息系统密码应用测评要求》中，关于密码应用技术测评要求的测评实施，其中测评实施第一条会关联到其他哪些测评单元（）。	通用测评要求的“密码算法合规性”	通用测评要求的“密码产品合规性”	通用测评要求的“密码技术正确性”	通用测评要求的“密码技术合规性”
3611	多项选择题	在GM/T 0115《信息系统密码应用测评要求》中，关于密码应用技术测评要求的测评实施，其中测评实施第二条会关联到其他哪些测评单元（）。	通用测评要求的“密码算法合规性”	通用测评要求的“密码产品合规性”	通用测评要求的“密码服务合规性”	通用测评要求的“密钥管理安全性”
3612	多项选择题	某三级信息系统机房有A和B两个门，经实地查看发现，无论从A或B门进入后，都可以访问整个机房。其中A门采用经检测认证的电子门禁系统刷卡进入，B门采用ID卡刷卡进入。对机房进出访问无其他风险控制措施。针对这种情形，依据GM/T 0115《信息系统密码应用测评要求》，物理和环境安全层面“身份鉴别”的判定结果和风险评价最有可能的是（）。	部分符合	不符合	高风险	无风险
3613	多项选择题	在GM/T 0115《信息系统密码应用测评要求》中，在测评到某信息系统的网络和通信安全层面时，密评人员可以选取以下哪些选项作为该安全层面的测评对象（）。	异地办事人员访问该系统产生的VPN通信信道	该系统生产机房和数据灾备机房之间的通信信道（两个机房位于不同城市）	运维人员从办公网区域访问安全运维区的堡垒机而产生的设备运维管理通道（两个区域同属于单位内网）	该系统移动端APP访问服务端建立的HTTPS通信信道

3614	多项选择题	在GM/T 0115《信息系统密码应用测评要求》中，针对“投入运行前进行密码应用安全性评估”这一项测评指标，以下说法正确的是（ ）。	对于第一级和第二级的信息系统，密评人员应核查信息系统投入运行前是否组织进行密码应用安全性评估，且编制有密码应用安全性评估报告	对于第二级和第三级的信息系统，密评人员应核查信息系统投入运行前是否组织进行密码应用安全性评估，并核查是否编制有密码应用安全性评估报告且系统通过评估	对于所有级别的信息系统，密评人员应核查信息系统投入运行前是否组织进行密码应用安全性评估，并核查是否编制有密码应用安全性评估报告且系统通过评估	对于第三级和第四级的信息系统，密评人员应核查信息系统投入运行前是否组织进行密码应用安全性评估，并核查是否编制有密码应用安全性评估报告且系统通过评估
3615	多项选择题	密评人员在测评某三级信息系统时发现，该系统数据加密密钥的管理采用了一台服务器密码机实现，但该密码机对应的认证证书在测评时已过期（系统方采购密码机时间在认证证书有效期内）。针对这种情形，依据GM/T 0115《信息系统密码应用测评要求》，“密钥管理安全性”可能的判定结果有哪些（ ）。	符合	不符合	不适用	以上都有可能
3616	多项选择题	根据GM/T 0115《信息系统密码应用测评要求》附录B，在密评中对密码机可采用以下哪些测评技术（ ）。	利用协议分析工具，抓取应用系统调用密码机的指令报文，验证其是否符合预期（如调用频率是否正常、调用指令是否正确）	管理员登录密码机查看相关配置，检查内部存储的密钥是否对应合规的密码算法，密码计算时是否使用合规的密码算法等	在模拟的主机或抽选的主机上安装监控软件（如Bus Hound），抓取和分析密码机的APDU指令，确认调用指令格式和内容符合预期	管理员登录密码机查看日志文件，根据与密钥管理、密码计算相关的日志记录，检查是否使用合规的密码算法等

3617	多项选择题	根据GM/T 0115《信息系统密码应用测评要求》附录B，在密评中对动态口令系统可采用以下哪些测评技术（ ）。	尝试对动态口令进行重放，以确认重放后的口令无法通过认证系统的验证	条件允许情况下，确认种子密钥以密文形式导入至认证系统中	条件允许情况下，在动态口令计算完成后，确认明文种子密钥不会留存在认证系统中	判断动态令牌的PIN码保护机制是否符合相关密码产品技术标准要求，例如PIN码长度、输入错误次数限制
3618	多项选择题	根据GM/T 0115《信息系统密码应用测评要求》，在对物理和环境安全层面“身份鉴别”指标进行测评时，可采用的方法包括（ ）。	尝试发一些错误的门禁卡，验证这些卡无法打开门禁	利用发卡系统分发不同权限的卡，验证非授权的卡无法通过门禁验证	查看电子门禁系统后台密码算法配置，确认用于门禁身份鉴别的密码算法合规性	通过抓取电子门禁系统后台与门禁日志记录审计系统的通信数据，确认门禁日志记录的完整性保护措施
3619	多项选择题	根据GM/T 0115《信息系统密码应用测评要求》，下列哪些密码技术能够满足保护电子门禁系统进出记录数据的存储完整性（ ）。	基于对称密码算法的MAC技术	基于密码杂凑算法的MAC技术	对称加密	SM2数字签名
3620	多项选择题	根据GM/T 0115《信息系统密码应用测评要求》，下面哪些密码技术能够满足保护视频监控记录数据的存储完整性（ ）。	基于对称密码算法的MAC技术	对称加密	基于密码杂凑算法的MAC技术	SM2数字签名
3621	多项选择题	依据GM/T 0115《信息系统密码应用测评要求》，对网上银行系统进行测评时，客户端与其后台系统进行通信过程中，使用下列哪些密码套件可以判定“密码算法合规性”“密码技术合规性”这两项为“符合”（ ）。（假定通信两端所采用的密码产品均经过检测认证）	ECC_SM4_SM3	RSA_SM4_SM3	ECDHE_SM4_SM3	RSA_AES256_SHA384

3622	多项选择题	某应用系统部署在单位内网服务器区，内部办公区用户通过局域网访问应用系统，外部用户通过互联网访问应用系统，运维管理员可以从互联网先登录运维SSL VPN网关后，再通过SSL VPN网关堡垒机对服务器、密码产品等设备进行运维，也可以从机房内的运维终端直接通过管理网对设备进行运维。依据GM/T 0115《信息系统密码应用测评要求》，下面哪些通信信道可作为网络和通信安全的测评对象（ ）。	内部办公区用户终端与应用系统之间的通信信道	外部互联网用户终端与应用系统之间的通信信道	机房内的运维终端与被管理设备之间的通信信道	互联网运维管理员终端与SSL VPN之间的通信信道
3623	多项选择题	根据GM/T 0115《信息系统密码应用测评要求》中对“建立密码应用岗位责任制度”的要求，在测评某三级信息系统时，发现以下哪些情况会判定为不符合关于“互相制约、互相监督”的要求（ ）。	密码安全审计员兼任密钥管理员	密钥管理员兼任密码操作员	关键安全岗位仅设置密钥管理员和密码操作员，而且由同一人兼任	密码安全审计员兼任密码操作员
3624	多项选择题	根据GM/T 0115《信息系统密码应用测评要求》，在对某二级信息系统进行“建立上岗人员培训制度”指标的测评时，下列哪些可能成为核查的对象（ ）。	人员培训管理制度	培训计划	培训签到表	安全教育类文档
3625	多项选择题	根据GM/T 0115《信息系统密码应用测评要求》，在测评某三级信息系统“定期进行安全岗位人员考核”指标时，应核查的内容包括（ ）。	核查安全管理制度文档是否包含具体的人员考核制度和惩戒措施	核查人员考核记录内容是否包括安全意识、密码操作管理技能及相关法律法规	核查人员是否具有外部培训的记录	核查记录表单类文档以确认是否定期进行岗位人员考核
3626	多项选择题	依据GM/T 0115《信息系统密码应用测评要求》，密评人员在进行人员管理方面的测评时，应核查是否定期对密码应用安全岗位人员进行考核，查看人员考核记录内容是否包括（ ）。	制定密码应用方案	安全意识	相关法律法规	密码操作管理技能

3627	多项选择题	某信息系统部署了同一生产厂商的4台应用服务器，其中，2台型号为A，操作系统版本分别为C，2台型号为D，操作系统版本分别为E、F；2台服务器密码机（商用密码产品认证证书编号分别为GMxxx、GMyyy）；以下关于设备和计算安全层面测评对象选取的做法中，错误的是（ ）。	从4台应用服务器抽选1台作为测评对象，从2台服务器密码机抽选1台作为测评对象	从不同型号的应用服务器分别抽选1台作为测评对象，2台服务器密码机分别作为测评对象	4台应用服务器分别作为测评对象，2台服务器密码机也分别作为测评对象	从不同操作系统版本的应用服务器抽选1台作为测评对象，2台服务器密码机分别作为测评对象
3628	多项选择题	根据GM/T 0115《信息系统密码应用测评要求》，关于密钥生存周期管理检查要点，以下说法正确的是（ ）。	确认密钥是否在经检测认证合格的密码产品中产生，核实密钥产生功能的正确性和有效性	确认密钥（含公钥）存储过程中使用了哪些密码技术对密钥进行处理以保护其机密性，并核实保护措施使用的正确性和有效性	核实归档密钥是否仅用于解密被加密的历史信息或验证被签名的历史信息	核实密钥销毁过程和销毁方式，保证密钥销毁后是可以被恢复的
3629	多项选择题	某信息系统管理员从互联网通过SSL VPN接入内网后，登录堡垒机对应用服务器进行集中管理，应用用户从互联网访问应用系统。依据GM/T 0115《信息系统密码应用测评要求》，设备和计算安全层面“远程管理通道安全”测评指标涉及的传输通道包括（ ）。	从互联网到SSL VPN网关的通信信道	接入内网后访问堡垒机的通道	通过堡垒机对应用服务器进行管理的通道	互联网访问应用系统的通道
3630	多项选择题	根据GM/T 0115《信息系统密码应用测评要求》，以下可作为设备和计算安全层面“远程管理通道安全”测评内容的是（ ）。	管理员从互联网使用浏览器直接访问堡垒机管理应用的通道	管理员在互联网通过SSL VPN接入内网后，使用浏览器访问堡垒机管理应用的通道	管理员在内网通过堡垒机对应用服务器进行集中管理的通道	业务用户在互联网使用国密浏览器访问业务应用的通道

3631	多项选择题	根据GM/T 0115《信息系统密码应用测评要求》，下列关于应用和数据安全层面测评的说法中不正确的是（ ）。	如果被测信息系统无密码应用方案，本安全层面的测评对象可访谈设备管理相关人员了解情况	依据GM/T 0115《信息系统密码应用测评要求》，任何情况下，二级信息系统都不必进行“不可否认性”测评	某应用系统所在服务器自身不含有用于身份鉴别的软件密码模块，则“身份鉴别”指标为不适用	应用系统采用了未经安全性验证的自研密码算法对重要数据进行存储机密性保护，密评人员现场确认重要数据非明文存储，可判定为“部分符合”
3632	多项选择题	根据GM/T 0115《信息系统密码应用测评要求》，在对应用和数据安全层面中的“身份鉴别”指标测评时，应用系统采用以下（ ）密码技术可能被判定为“符合”或“部分符合”。	采用SM4算法生成动态口令	基于MD5的RSA-2048数字签名	SM3-HMAC	基于SHA-256的SM2数字签名
3633	多项选择题	根据GM/T 0115《信息系统密码应用测评要求》，在移动办公场景下，经访谈了解到手机端移动OA办公平台APP集成了手机盾SDK，应用服务端部署协同签名平台对办公用户采用基于SM2数字证书的协同签名技术实现身份鉴别，则应用和数据安全层面“身份鉴别”指标测评方法通常包括（ ）。	核查移动终端密码模块、协同签名平台是否经商用密码认证机构认证合格	核查APP用户数字证书格式合规性和数字证书有效性	核查APP用户数字证书颁发机构是否获得了密码管理部门颁发的《电子认证服务使用密码许可证》	核查应用服务端是否如实调用协同签名平台进行签名验证
3634	多项选择题	被测对象为某网上银行系统，依据GM/T 0115《信息系统密码应用测评要求》,应用和数据安全层面“身份鉴别”测评要点包括（ ）。	核查网银应用管理员用户登录网上银行系统时是否采用密码技术进行身份鉴别，并验证身份鉴别机制的正确性和有效性	核查网银用户登录网上银行系统后，进行关键交易时是否对关键信息进行签名，并验证签名的正确性和有效性	核查身份鉴别采用的密码算法、密码技术、密码产品和密码服务是否合规	在密码产品、密码服务合规的前提下，还应进一步核查密钥管理安全性实现技术是否正确有效

3635	多项选择题	被测业务应用系统采用基于角色的访问控制策略，用户通过角色配置获得该角色拥有的应用系统权限，在对该应用系统进行应用和数据安全层面“访问控制信息完整性”测评时，依据GM/T 0115《信息系统密码应用测评要求》，从理论上可采取的实施方法包括（ ）。	读取数据库中的用户角色配置信息，判断完整性校验值的格式是否符合预期	读取数据库中的角色权限配置信息，判断完整性校验值的格式是否符合预期	如使用数字签名技术进行完整性保护，则可使用公钥对存储的签名结果进行验证	如使用消息鉴别码进行完整性保护，则可使用完整性保护密钥对存储的MAC值进行验证
3636	多项选择题	根据GM/T 0115《信息系统密码应用测评要求》，应用和数据安全层面“重要数据传输机密性”的测评实施要点描述正确的是（ ）。	依据GM/T 0115《信息系统密码应用测评要求》，还会进行通用测评要求的核查	利用协议分析工具，分析传输的重要数据是否为密文，数据格式（如分组长度等）是否符合预期	使用密码算法合规性验证工具对抓取的密文数据进行验签，并与明文进行对比，以验证密码算法是否与声称的一致	如采用IPSec协议保障数据传输安全，利用协议分析工具捕获并分析握手阶段Server hello消息数据包
3637	多项选择题	根据GM/T 0115《信息系统密码应用测评要求》，在对应用和数据安全层面中的“重要数据传输机密性”指标测评时，经核查测评对象采取下列哪些措施时，可能导致机密性保护是无效（ ）。	采用RSA-1024公钥加密的方式对口令信息进行传输保护	身份证号的后六位采用“*”代替后进行传输	同一类重要业务数据在某一传输通道中明文传输，在其他传输通道中密文传输	采用DES算法进行加密传输
3638	多项选择题	根据GM/T 0115《信息系统密码应用测评要求》，业务应用系统调用服务器密码机，采用对称密码算法对重要数据进行存储机密性保护，在对重要数据进行应用和数据安全层面“重要数据存储机密性”指标测评时，可采取的测评方法包括（ ）。	登录数据库查看存储的重要数据是否非明文存储	管理员登录服务器密码机查看日志文件，根据与密钥管理、密码计算相关的日志记录，检查是否与声称的一致	登录数据库查看存储的重要数据密文格式（如密文长度）是否符合预期密码算法特征	抓取应用系统调用服务器密码机的指令报文，验证其是否符合预期(如调用频率是否正常、调用指令是否正确)
3639	多项选择题	根据GM/T 0115《信息系统密码应用测评要求》，在对三级信息系统进行应用和数据安全层面“重要数据存储机密性”指标测评时，预期结果包括（ ）。	重要数据为密文存储，且数据格式符合预期	若调用外接密码产品实现，调用指令、次数等符合预期	密钥配置、日志记录均显示使用合规的密码算法	采用的密码产品具有密码管理部门颁发的密码服务许可文件

3640	多项选择题	根据GM/T 0115《信息系统密码应用测评要求》，应用和数据安全层面“重要数据传输完整性”的测评实施要点包括（）。	该测评单元的实施项中第一条和第二条涉及通用测评要求的密码算法合规性、密码技术合规性、密码产品合规性和密码服务合规性四个方面	利用协议分析工具，分析受完整性保护的数据在传输时的数据格式（如签名长度、MAC长度）是否符合预期	如果使用数字签名技术进行完整性保护，可使用公钥对抓取的签名结果进行验证	如果以外接服务器密码机等密码产品的形式实现，需要核实密码产品是否如实被调用
3641	多项选择题	业务应用系统调用签名验签服务器，采用数字签名技术对重要数据进行存储完整性保护，在对重要数据进行应用和数据安全层面“重要数据存储完整性”指标测评时，依据GM/T 0115《信息系统密码应用测评要求》，可采取的测评方法包括（）。	登录数据库查看重要数据签名值长度是否符合预期	登录签名验签服务器查看日志文件，根据与密钥管理、密码计算相关的日志记录，检查是否与声称的一致	生成测试数据，尝试对测试数据进行篡改，验证完整性校验机制是否有效	抓取应用系统调用签名验签服务器的指令报文，验证其是否符合预期(如调用顿率是否正常、调用指令是否正确)
3642	多项选择题	依据GM/T 0115《信息系统密码应用测评要求》，在云平台测评中，下列哪些资产有可能作为应用和数据安全层面的测评对象（）。	云资源管理系统	密码服务平台	云上应用	统一身份认证平台
3643	多项选择题	车联网OTA（在线升级）业务场景中，智能网联汽车首先接入某运营商网络，然后与OTA云平台（云上应用系统）建立网络通信信道，下载OTA升级包到车端以完成软固件升级工作。根据上述所描述的OTA升级场景，依据GM/T 0115《信息系统密码应用测评要求》，密评时的关注点有以下哪些（）	OTA平台与智能网联汽车的网络通信实体鉴别	OTA升级包从车企到OTA平台的重要数据传输完整性保护	车端下载的OTA升级包的来源真实性和传输完整性	智能网联汽车接入运营商网络的安全认证

3644	多项选择题	根据GM/T 0115《信息系统密码应用测评要求》附录C，在密评中对“真实性”的测评技术，下列描述正确的是（ ）。	对于采用“挑战-响应”方式的鉴别协议，若通信双方有双向鉴别安全需求，那么按GB/T 15843相关要求，密评人员在分析协议数据包时，应确认用于实现双向鉴别的消息传递次数至少是四次	对于采用“挑战-响应”方式的鉴别协议，若通信双方有双向鉴别安全需求，那么按GB/T 15843相关要求，密评人员在分析协议数据包时，应确认用于实现双向鉴别的消息传递次数至少是三次	对于基于静态口令的鉴别过程，可通过抓取鉴别过程的数据包，确认口令未以明文形式传递	若采用基于SM2数字证书方式实现身份鉴别，除了验证签名结果外，还需要对相关数字证书进行验证
3645	多项选择题	根据GM/T 0115《信息系统密码应用测评要求》附录C，在密评中对“传输完整性”的测评技术，下列描述正确的是（ ）。	若该密码功能采用HMAC-SM3实现，可利用协议分析工具捕获受完整性保护的数据在传输过程中的数据包，并进一步分析MAC长度是否为256比特或更短	若该密码功能采用HMAC-SHA1实现，可利用协议分析工具捕获受完整性保护的数据在传输过程中的数据包，并进一步分析MAC长度是否为128	若该密码功能采用基于SM2数字签名技术实现，可利用协议分析工具捕获受完整性保护的数据在传输过程中的数据包，并进一步分析签名值长度是否为512比特	若该密码功能采用基于SM2数字签名技术实现，可使用给相应签名证书签发的CA的公钥对签名结果进行签名验证
3646	多项选择题	根据GM/T 0115《信息系统密码应用测评要求》，针对网络和通信安全层面“身份鉴别”指标的测评，下列哪些可能是测评时的考查点（ ）。	通过访谈安全管理员并查验设备是否获得了商用密码产品认证证书	通过抓包分析握手过程，解析密码算法或密码套件标识可判断采用的密码算法是否符合要求	通过抓包分析握手过程，解析通信实体使用的数字证书，判断采用的密码算法是否符合要求	通过验证测试可以判断身份鉴别机制是否正确有效

3647	多项选择题	根据GM/T 0115《信息系统密码应用测评要求》，针对网络和通信安全层面“通信数据完整性”指标的测评，下列哪些说法是正确的（ ）。	通过验证测试发现，可以使用工具修改请求数据包的内容得到想要的响应，因此判断本通信信道不能保证通信数据完整性	通过验证测试发现，无法修改请求数据包，但可以进行重放攻击，因此判断本通信信道不能保证通信数据完整性	通过对SSL握手阶段的抓包分析，使用的密码套件中算法全部为国密算法，但依然无法判断本通信信道是否可以保证通信数据完整性	通过对SSL握手阶段的抓包分析，获得的服务端的SM2签名证书为可信第三方CA机构颁发的，因此判断本通信信道能保证通信数据完整性
3648	多项选择题	根据GM/T 0115《信息系统密码应用测评要求》，针对网络和通信安全层面“通信过程中重要数据的机密性”指标的测评，下列哪些说法是正确的（ ）。	通过抓取通信过程的数据包，可以发现存在重要数据为明文，因此判断本通信信道不能保证通信过程中重要数据的机密性	通过核查发现本通信信道使用的VPN设备不具有商用密码产品认证证书，因此判断本通信信道一定不能保证通信过程中重要数据的机密性	通过对SSL握手阶段的抓包分析，获得的服务端的SM2加密证书为可信第三方CA机构颁发的，因此判断本通信信道能保证通信数据机密性	通过对SSL握手阶段的抓包分析，使用的密码套件为国外密码算法，但能判断本通信信道是否保证通信数据完整性
3649	多项选择题	根据GM/T 0115《信息系统密码应用测评要求》，针对网络和通信安全层面“网络边界访问控制信息的完整性”指标的测评，下列哪些说法是正确的（ ）。	某通信信道使用IPSec VPN进行网络边界访问控制，IPSec VPN获得了商用密码产品认证证书，通过IPSec VPN自身的安全机制可以保证访问控制信息的完整性	某通信信道通过防火墙进行网络边界访问控制，采用服务器密码机对访问控制信息计算MAC后保存，服务器密码机获得了商用密码产品认证证书，因此可以实现网络边界访问控制信息的完整性保护	某通信信道通过边界路由进行网络边界访问控制，并采用自实现的HMAC-SM3对访问控制信息计算MAC后保存，因此可以实现网络边界访问控制信息的完整性保护	通过核查发现，某网络边界设备的访问控制信息采用SM4-ECB算法加密后保存在硬盘中，因此可以判断该设备能够保证访问控制信息的完整性

3650	多项选择题	某信息系统管理员在内网使用浏览器访问堡垒机管理应用，浏览器与堡垒机之间的传输协议为HTTPS，依据GM/T 0115《信息系统密码应用测评要求》，以下说法正确的是（ ）。	HTTPS签名证书中签名算法OID为1.2.156.10197.1.501，测评人员由此可判定签名算法为SHA256WithRSA2048	测评人员可从HTTPS签名证书中获取使用者公钥	测评人员可通过上级CA证书对HTTPS签名证书的签名值进行验签	HTTPS协议算法套件标识为{0xe0,0x13}，测评人员由此可判定HTTPS协议算法套件为ECDHE_SM4_SM3
3651	多项选择题	在下列身份鉴别应用场景中，根据GM/T 0115《信息系统密码应用测评要求》，该测评对象在应用和数据安全层面“身份鉴别”测评指标可能被判定为“符合”的是（ ）。	WEB端业务用户使用手机APP客户端扫码登录业务应用系统，手机APP客户端集成手机盾SDK，服务端部署协同签名平台，采用SM2协同签名算法对登录用户进行身份鉴别	WEB端业务用户使用蓝牙型智能密码钥匙作为登录应用系统的凭证，服务端调用签名验签服务器进行签名验证	移动端业务用户使用动态令牌作为登录APP应用的凭证，服务端部署动态口令认证系统进行身份验证	政务服务系统个人用户通过省统一政务服务门户进行用户身份鉴别，省统一政务服务门户提供微信/支付宝扫码登录、手机验证码登录两种鉴别方式
3652	多项选择题	根据GM/T 0115《信息系统密码应用测评要求》，下列关于应用和数据安全层面“身份鉴别”指标测评实施说法错误的是（ ）。	若未采用数字证书对应用系统用户登录进行身份鉴别，则需要验证公钥或对称密钥与实体的绑定方式是否可靠	若采用数字证书对应用系统用户登录进行身份鉴别，且采用了合规的密码产品和密码服务，则通用要求中“密钥管理安全”可直接判定为符合	若采用智能密码钥匙作为用户登录凭证，智能密码钥匙的口令长度和错误口令登录验证次数无需在应用和数据安全层面考虑	不能复用密码产品检测结果时，需要核查实体鉴别协议是否符合GB/T 15843的要求

3653	多项选择题	某应用系统通过主客代理模块对数据和用户进行标记，实现基于安全标记的强制访问控制，在对该应用系统进行应用和数据安全层面“重要信息资源安全标记完整性”测评时，了解到信息系统内仅部署了一台服务器密码机提供密码运算支撑。依据GM/T 0122《信息系统密码应用测评要求》，经进一步核查，该测评单元可能的测评结果有（）。	符合	部分符合	不符合	不适用
3654	多项选择题	依据GM/T 0124《信息系统密码应用测评要求》，在下列重要数据传输机密性保护场景中，经整体测评后，应用和数据安全层面“重要数据传输机密性”测评结果可能为“符合”或“部分符合”的是（）。	客户端非国密浏览器与应用服务端采用TLS1.2协议，密码套件选用TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256	客户端浏览器使用服务端RSA(2048)公钥证书对鉴别数据进行加密（JavaScript实现）后传输	重要业务数据通过纯物理传输的裸光纤以明文方式备份至同城灾备机房	手机端使用TF密码卡对APP鉴别数据、重要业务数据进行SM4-GCM加密后传输，服务端调用服务器密码机解密重要数据
3655	多项选择题	GM/T 0129《信息系统密码应用测评要求》，在对应用和数据安全层面中的“重要数据存储机密性”指标测评时，以下哪些措施可能导致数据泄露（）。	采用DES算法对用户敏感信息加密后存储	调用服务器密码机采用SM4-ECB模式对所有用户性别信息项进行加密后存储	采用SM3（加盐）的方式对数据库中存储的口令信息处理	对重要用户信息进行脱敏后存储，未采用其他数据存储安全加固措施
3656	多项选择题	GM/T 0134《信息系统密码应用测评要求》，在测评应用和数据安全层面“重要数据存储完整性”指标时，获取到下列哪些证据即可判定测评对象不符合该项测评指标要求（）。	调用服务器密码机采用SM3算法计算重要用户信息杂凑值，并保存在数据库中	调用服务器密码机采用SM4-GCM对个人敏感信息进行存储机密性和完整性保护	调用签名验签服务器对重要业务数据进行SM2数字签名，签名值保存在数据库中，未设置签名校验机制	使用加密数据库系统存储重要业务数据

3657	多项选择题	GM/T 0137《信息系统密码应用测评要求》，某涉及法律责任认定的应用系统采用电子签章系统实现重要行为的不可否认性，在进行应用和数据安全层面“不可否认性”第三级指标测评时，测评要点包括但不限于（ ）。	核查电子签章系统是否具有商用密码产品认证证书，且密码模块安全等级为二级及以上	核查电子印章载体是否合规	核查制章人和签章人数字证书格式、签名算法标识和颁发机构	核查电子印章的验证、电子签章的生成和验证是否符合GB/T 38540的要求
3658	多项选择题	某信息系统部署了经检测认证的签名验签服务器，且密码模块达到了相应等级要求，关于设备和计算安全层面应用服务器“系统资源访问控制信息完整性”测评项，依据GM/T 0115《信息系统密码应用测评要求》，以下判定结果错误的是（ ）。	通过调用签名验签服务器的AES-128 ECB模式加密接口，对访问控制信息加密，取最后一组分组密文作为MAC并存储，值为A；在验证完整性时，调用签名验签服务器的AES-128 ECB模式加密接口，对访问控制信息加密，取最后一组分组密文作为MAC，值为B，比对A与B是否一致；基于上述措施，测评人员判定为部分符合	通过调用签名验签服务器的SM4 CBC-MAC接口，对访问控制信息计算MAC并存储，值为A；在验证完整性时，调用签名验签服务器SM4 CBC-MAC接口，对访问控制信息计算MAC，值为B，比对A与B是否一致；其中，计算SM4 CBC-MAC使用的初始向量为符合密码相关国家和行业标准的随机数；基于上述措施，测评人员判定为符合	通过调用签名验签服务器的SM3接口，计算访问控制信息的杂凑值并存储，值为A；在验证完整性时，调用签名验签服务器SM3接口，计算访问控制信息的杂凑值，值为B，比对A与B是否一致；基于上述措施，测评人员判定为不符合	通过调用签名验签服务器的HMAC-SHA256接口，对访问控制信息计算MAC并存储，值为A；在验证完整性时，将访问控制信息与A拼接，并调用签名验签服务器HMAC-SHA256接口，对拼接数据计算MAC，值为B，比对A与B是否一致；基于上述措施，测评人员判定为部分符合

3659	多项选择题	某信息系统在国密改造实施技术文档中标明，采用SM2签名验签的机制对应用服务器日志记录进行完整性保护，并采用HMAC-SM3算法对系统资源访问控制信息进行完整性保护，两名密码操作员可使用智能密码钥匙登录签名验签服务器，依据GM/T 0115《信息系统密码应用测评要求》，以下关于测评人员在测评实施中，属于错误判定的是（ ）。	测评人员经核查发现，系统实际存储SM2签名的字段值长度为256位，因此判定日志记录完整性保护可能未使用SM2签名验签机制	测评人员经核查发现，系统实际存储HMAC-SM3的字段值长度为128位，因此判定系统资源访问控制信息完整性保护使用的不是HMAC-SM3算法	测评人员经核查发现，智能密码钥匙设置的口令长度不小于6个字符，使用错误口令登录的次数限制不超过10次，因此判定智能密钥钥匙的口令相关设置不符合GM/T 0027的要求	测评人员经核查发现，两名密码操作员都使用了合规CA机构签发的同一张数字证书，证书在有效期内，且进行了证书的有效性验证，因此判定数字证书的签发和使用符合密评相关标准要求
3660	多项选择题	依据GM/T 0115《信息系统密码应用测评要求》，以下关于测评人员在设备和计算安全层面测评实施过程中，正确的是（ ）。	某信息系统访问堡垒机管理应用的远程管理通道使用了HTTPS协议，算法套件为TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA；测评人员判定用于通信数据完整性保护的算法为CBC-MAC-AES-256	某信息系统访问堡垒机管理应用的远程管理通道使用了HTTPS协议，测评人员经核查发现HTTPS数字证书在有效期内，并使用该证书内的公钥对证书签名值进行验签，验签不通过；测评人员判定该证书为无效证书	某信息系统管理员在互联网直接访问堡垒机对设备进行管理；测评人员将访问堡垒机的通信信道作为设备和计算安全层面“远程管理通道安全”的测评对象	某信息系统部署和使用了2台SSL VPN网关，商用密码产品认证证书编号分别为GMxxx、GMyyy;测评人员将2台SSL VPN网关分别作为设备和计算安全层面的两个测评对象

3661	多项选择题	某三级信息系统于2023年进行首次密评，系统于2018年9月正式投入运行，系统责任单位未制定密码应用方案（或改造方案）和实施方案，密钥管理制度及策略文档中标明非对称密钥对在服务器密码机中进行存储，并且非对称密钥对在数据库服务器进行明文备份，依据GM/T 0115《信息系统密码应用测评要求》，以下关于建设运行层面的判定，正确的是（ ）。	测评人员判定“制定密码应用方案”测评项为不符合	测评人员判定“投入运行前进行密码应用安全性评估”测评项作为不适用	测评人员判定密钥管理及策略文档不存在安全问题	测评人员判定“制定实施方案”测评项为部分符合
3662	多项选择题	依据GM/T 0115《信息系统密码应用测评要求》，以下关于设备和计算安全层面“身份鉴别”测评项的判定，错误的是（ ）。	某信息系统管理员使用用户名+口令或使用经检测认证的智能密码钥匙（密码模块达到相应等级要求）登录签名验签服务器，口令使用加盐SHA256算法进行传输和存储保护，测评人员判定签名验签服务器“身份鉴别”测评项为部分符合	某信息系统管理员使用经检测认证的智能密码钥匙（密码模块达到相应等级要求）登录堡垒机，身份鉴别机制符合GB/T 15843标准要求，测评人员判定堡垒机“身份鉴别”测评项一定为符合	某信息系统管理员使用智能密码钥匙登录堡垒机，测评人员发现智能密码钥匙换发的商用密码产品认证证书中未标注密码模块安全等级，测评人员判定智能密码钥匙仅符合一级密码模块要求	某信息系统管理员使用动态令牌登录堡垒机，测评人员经核查发现，动态令牌设置的PIN码长度不少于6位数字，PIN码尝试次数最大不可超过8次；测评人员判定PIN码相关设置不符合GB/T 38556的要求
3663	多项选择题	某信息系统管理员使用智能密码钥匙登录签名验签服务器，对管理员进行身份鉴别，身份鉴别机制采用数字签名技术，并基于“挑战-响应”鉴别机制。依据GM/T 0115《信息系统密码应用测评要求》，在上述场景下，以下关于该机制的实现方式，错误的是（ ）。	通过智能密码钥匙产生随机数，并检验该随机数来保证唯一性和时效性	智能密码钥匙产生并向签名验签服务器发送Token	签名验签服务器产生的挑战值“随机数”未包含在Token签名数据中	由智能密码钥匙解密私钥对签名数据进行签名，并由签名验签服务器验签

3664	多项选择题	某信息系统设备和计算安全层面，通过SM2签名验签的方式对应用服务器的日志记录进行完整性保护，测评人员提取了4组十六进制字符串的SM2签名值，以下SM2签名值符合GM/T 0009签名数据格式要求的是（ ）。	0x304402202DB887AB6768A70E9F13597BDDEBB4B16B284A8CF51DF21BCFC16B6FADC84FB70220531B8EB27F12738980E5687D56663AC27D196822E3277F1E68C8456EC206D5D0	0x042DB887AB6768A70E9F13597BDDEBB4B16B284A8CF51DF21BCFC16B6FADC84FB7531B8EB27F12738980E5687D56663AC27D196822E3277F1E68C8456EC206D5D0	0x30450220390E325EB7CF7BABA3698839A739DCE23504CE058597FB5931CF11154B3BB0D9022100BE9C6210A2D9984 0778F7E9781B8AABD1CA9060068F38902394B7A4693530F1B	0x04390E325EB7CF7BABA3698839A739DCE23504CE058597FB5931CF11154B3BB0D9BE9C6210A2D99840778F7E9781B8AABD1CA9060068F38902394B7A4693530F1B
3665	多项选择题	某信息系统基于开源算法库实现国密HTTPS协议，测评人员获取了系统存储的SM2签名私钥文件（符合ASN.1编码）和签名证书，依据GM/T 0115《信息系统密码应用测评要求》，关于密钥管理安全性分析思路，以下说法正确的是（ ）。	参考PKCS#8规范可分析该私钥文件为明文结构或密文结构	若该私钥文件为符合PKCS#8规范的明文结构，可验证私钥结构中私钥是否符合GB/T 35275中的私钥语法格式	通过数字证书格式合规性检测工具可验证私钥结构的合规性	若私钥结构中私钥符合GB/T 35275中的私钥语法格式，可从中提取私钥有效值，并通过密码算法合规性检测工具验证SM2私钥和公钥的匹配性
3666	多项选择题	某信息系统使用HMAC-SM3算法对设备和计算安全层面日志记录进行完整性保护。使用SM4算法对HMAC-SM3密钥进行加密存储，SM4密钥存储在配置文件中；对HMAC-SM3密钥进行杂凑运算，并存储杂凑值，其中，已知杂凑值的长度为32字节，值为0x3b366d29964b5543be7aa7cc064f9eeef9481baaa656c8bd3a88b431a8fb6f6c，以下说法正确的是（ ）。	测评人员由此可判定对HMAC-SM3密钥进行杂凑运算的杂凑算法不是SHA-1	测评人员由此可判定HMAC-SM3密钥管理合规、正确	测评人员由此可判定对HMAC-SM3进行杂凑运算的杂凑算法可能为SHA-256	测评人员由此可判定对HMAC-SM3进行杂凑运算的杂凑算法可能为SM3

3667	多项选择题	某三级信息系统管理员从互联网使用“用户名+口令+智能密码钥匙”登录VPN网关，智能密码钥匙的密码模块安全等级为一级，通过SSL VPN接入内网后，使用“用户名+口令+短信验证码”登录堡垒机管理应用，并对应用服务器进行运维管理，依据GM/T 0115《信息系统密码应用测评要求》，以下说法正确的是（ ）。	测评人员由此可判定堡垒机的身份鉴别为部分符合	测评人员可将接入内网后访问堡垒机管理应用的通道作为设备和计算安全层面“远程管理通道安全”测评项的测评对象	测评人员由此可判定应用服务器的身份鉴别为部分符合	测评人员由此可判定智能密码钥匙密码模块安全等级未达到系统等级要求
3668	多项选择题	某信息系统应用服务器通过调用最新版OpenSSL密码算法库的HMAC-SM3接口对日志记录计算MAC，依据GM/T 0115《信息系统密码应用测评要求》，以下哪些HMAC-SM3算法输出长度，使设备和计算安全“日志记录完整性”指标可能是“部分符合”的判定结果（ ）。	128比特	256比特	384比特	512比特
3669	多项选择题	依据GM/T 0115《信息系统密码应用测评要求》，关于设备和计算安全层面的判定结果，以下说法正确的是（ ）。	某三级信息系统，采用经检测认证的服务器密码机，其密码模块等级为二级，调用其SM4-CBC模式的加密算法接口，对应用服务器的日志记录进行加密，测评人员判定该应用服务器“日志记录完整性”为不符合	某二级信息系统，采用经检测认证的签名验签服务器，其密码模块等级为一级，调用其SM3算法接口，对应用服务器的系统资源访问控制信息进行杂凑运算，测评人员判定该应用服务器“系统资源访问控制信息完整性”为不符合	某信息系统采用智能密码钥匙登录签名验签服务器，智能密码钥匙和签名验签服务器均经过检测认证，密码模块均达到了相应等级安全要求，并采用了符合GB/T 15843标准要求的身份鉴别机制，测评人员判定该签名验签服务器“身份鉴别”为符合	某三级信息系统部署了经检测认证的服务器密码机，其密码模块等级为二级，测评人员判定服务器密码机“身份鉴别”为符合

3670	多项选择题	依据GM/T 0115《信息系统密码应用测评要求》，关于设备和计算安全层面的判定结果，以下说法正确的是（ ）。	某二级信息系统，系统责任方自行决定将“日志记录完整性”指标项不纳入标准符合性测评范围，测评人员将该项判定为“不适用”	某三级信息系统，制定了密码应用方案并通过了方案评估，方案评估意见中明确将“系统资源访问控制信息”指标项作为不适用，测评人员在实际测评时可直接将该项判定为“不适用”	某三级信息系统，制定了密码应用方案并通过了方案评估，方案评估意见中明确“重要可执行程序完整性、重要可执行程序来源真实性”指标项可采用方案中提供的风险控制措施完成，但测评人员在现场测评中发现方案中描述的风险控制措施使用条件并不满足，故此按照GM/T 0115相应的测评指标要求进行了测评和结果判定	若测评单元涉及多台通用设备作为测评对象，则测评人员可直接从中抽选测评对象，并进行测评实施和结果判定
3671	多项选择题	某信息系统设备和计算安全层面“身份鉴别”测评单元包含5个测评对象，依据GM/T 0115《信息系统密码应用测评要求》，以下判定结果正确的是（ ）。	若5个测评对象均为符合，则“身份鉴别”测评单元判定为符合	若其中2个测评对象为部分符合，3个测评对象为符合，则“身份鉴别”测评单元判定为部分符合	若其中2个测评对象为不符合，3个测评对象为符合，则“身份鉴别”测评单元判定为部分符合	若其中2个测评对象为不符合，3个测评对象为部分符合，则“身份鉴别”测评单元判定为不符合

3672	多项选择题	依据GM/T 0115《信息系统密码应用测评要求》，某业务应用系统在身份鉴别和不可否认性实现方面采用了数字证书，数字证书由经商用密码认证机构认证合格的证书认证系统签发，则密评人员在测评实施时需要（ ）。	参考GM/T 0037和GM/T 0038的要求核查证书认证系统部署是否正确、合规	核查证书扩展项KeyUsage字段，确定是否符合双证书体系要求，并验证证书及其相关私钥是否正确使用	核查Signature、Issuer等字段是否符合预期	通过数字证书格式合规性检测工具，验证证书格式是否符合GB/T 20518的有关要求
3673	多项选择题	网上行政审批系统主要提供审批业务受理、承办、审核、批准、结办等功能，其安全保护等级为三级；该单位内部用户采用SM2数字证书认证方式登录审批端业务应用，应用服务端调用签名验签服务器进行签名验证。依据GM/T 0115《信息系统密码应用测评要求》，在对单位内部用户进行应用和数据安全层面“身份鉴别”指标测评时，经核实发现下列（ ）情况可导致该测评指标无法取得“符合”的测评结果。	登录成功后，拔出智能密码钥匙，审批端业务应用长时间未自动退出登录	智能密码钥匙的商用密码产品认证证书和原型号证书中均未注明密码模块安全等级	SM2数字证书由本单位内部自建CA签发，组成CA的相关密码产品未经过检测认证	智能密码钥匙未导入SM2签名证书
3674	多项选择题	依据GM/T 0115《信息系统密码应用测评要求》，对物联网平台开展应用和数据安全层面测评时，根据其密码应用需求，需要针对下列哪些环节进行“身份鉴别”指标测评（ ）。	物联网终端接入	管理系统业务用户登录	管理系统运维用户登录	对感知节点设备上的软件应用进行配置或变更
3675	多项选择题	根据GM/T 0115《信息系统密码应用测评要求》，下列哪些属于第三级信息系统应急处置方面的测评实施要点（ ）。	访谈安全主管被测信息系统是否发生过密码应用安全事件	核查是否具有密码应用安全事件处置记录	核查管理制度或应急策略中是否明确规定事件发生后和事件处置完成后的上报机制	核查密码应用安全事件发生后是否向归属的密码管理部门提交了安全事件发生情况报告

3676	判断题	根据GM/T 0115《信息系统密码应用测评要求》，对于“可”的条款，由信息系统责任方自行决定是否按照GM/T 0115《信息系统密码应用测评要求》相应测评指标要求进行测评和结果判定。	正确	错误		
3677	判断题	根据GM/T 0115《信息系统密码应用测评要求》，对于“可”的条款，也存在测评指标“不适用”的情形。	正确	错误		
3678	判断题	根据GM/T 0115《信息系统密码应用测评要求》，对于“宜”的条款，密评人员无需参考方案评估意见，在测评时只需核实密码应用方案中所描述的风险控制措施是否落实即可。	正确	错误		
3679	判断题	信息系统是否涉及GM/T 0115《信息系统密码应用测评要求》中某项测评指标的安全需求，可通过是否采用密码技术实现该条款的安全防护加以判断。	正确	错误		
3680	判断题	在对某三级信息系统进行密评时，只要是GB/T 39786《信息安全技术 信息系统密码应用基本要求》中“应”的条款，则密评人员务必按照GM/T 0115《信息系统密码应用测评要求》中相应的测评指标要求进行测评和结果判定。	正确	错误		
3681	判断题	在GM/T 0115《信息系统密码应用测评要求》中，测评单元由测评指标、测评对象、测评实施这三个要素组成。	正确	错误		
3682	判断题	根据GM/T 0115《信息系统密码应用测评要求》，密码应用技术测评要求中的测评单元若涉及两个测评对象，则每个测评对象需要分别进行测评实施和结果判定，再汇总得出测评单元的结果。	正确	错误		

3683	判断题	根据GM/T 0115《信息系统密码应用测评要求》，整体测评环节要考虑单元间、对象间是否存在相互弥补的情况。	正确	错误		
3684	判断题	密评人员在执行GM/T 0115《信息系统密码应用测评要求》中的风险分析和评价环节时，可参考《信息系统密码应用高风险判定指引》。	正确	错误		
3685	判断题	根据GM/T 0115《信息系统密码应用测评要求》，信息系统的测评结论是由量化评估的得分以及风险分析和评价共同决定的。	正确	错误		
3686	判断题	依据GM/T 0115《信息系统密码应用测评要求》，被测信息系统有密码应用方案且方案通过评估，密码应用方案中明确“物理和环境安全”层面的测评指标为“不适用”。则根据密码应用方案和方案评估意见，密评人员无需对该层面进行测评，相应测评指标可直接判定为“不适用”。	正确	错误		
3687	判断题	依据GM/T 0115《信息系统密码应用测评要求》，某三级信息系统密码应用方案中网络和通信安全层面，“身份鉴别”指标要求验证通信双方身份鉴别的有效性，密评人员应按照密码应用方案的要求进行测评，并将结论体现在密评报告中。	正确	错误		
3688	判断题	根据GM/T 0115《信息系统密码应用测评要求》，密码算法合规性、密码技术合规性、密码产品合规性、密码服务合规性和密钥管理安全性不单独判定符合性，也不单独体现在密码应用安全性评估报告的单元测评结果和整体测评结果中。	正确	错误		

3689	判断题	依据GM/T 0115《信息系统密码应用测评要求》，经核查和验证某视频监控系统采用HMAC-SHA512算法（算法实现正确）来保证视频监控音像记录数据的存储完整性，因此“视频监控记录数据存储完整性”指标可判定为“部分符合”。	正确	错误		
3690	判断题	根据GM/T 0115《信息系统密码应用测评要求》，网络和通信安全层面的测评对象不包括信息系统内不同应用服务器之间的通信信道（在同一网段内）。	正确	错误		
3691	判断题	依据GM/T 0115《信息系统密码应用测评要求》，某三级信息系统，经核查和验证，网络通信信道采用了具有商用密码产品认证证书的SSL VPN设备，SSL协议使用的密码算法套件为ECC_SM4_SM3，因此判定该网络信道符合“通信数据完整性”和“通信过程中重要数据机密性”测评指标的要求。	正确	错误		
3692	判断题	依据GM/T 0115《信息系统密码应用测评要求》，在对“网络和通信安全”层面测评时，如果网络边界的访问控制信息存储在具有商用密码产品认证证书的VPN类设备中，则针对该层面“网络边界访问控制信息的完整性”指标可直接判定为“符合”。	正确	错误		
3693	判断题	依据GM/T 0115《信息系统密码应用测评要求》，在三级信息系统的测评中，针对“建立密码应用岗位责任制度”指标的测评，需要核查相关设备与系统的管理和使用账号是否存在多人共用的情况。	正确	错误		

3694	判断题	依据GM/T 0115《信息系统密码应用测评要求》，交换机、网闸、防火墙、WAF等未使用密码功能的网络设备、安全设备，一般可不作为设备和计算安全层面的测评对象。	正确	错误		
3695	判断题	依据GM/T 0115《信息系统密码应用测评要求》，在设备和计算安全层面，应将系统中全部的设备做为独立的测评对象进行测评和量化评估。	正确	错误		
3696	判断题	依据GM/T 0115《信息系统密码应用测评要求》，某信息系统通过堡垒机集中运维管理设备，而堡垒机前部署了合规的SSL VPN，管理员使用合规的身份鉴别机制登录SSL VPN，则在设备和计算安全层面，堡垒机的“身份鉴别”可判定为“符合”。	正确	错误		
3697	判断题	依据GM/T 0115《信息系统密码应用测评要求》，在设备和计算安全层面，堡垒机使用合规的智能密码钥匙实现身份鉴别，通用服务器、数据库通过堡垒机进行统一管理。若堡垒机的“身份鉴别”指标的测评结论为“符合”，则通用服务器的身份鉴别可判定为“符合”。	正确	错误		
3698	判断题	依据GM/T 0115《信息系统密码应用测评要求》，，某信息系统通过堡垒机对系统中的通用服务器进行统一运维管理，若堡垒机使用合规的智能密码钥匙实现身份鉴别，则在设备和计算安全层面“身份鉴别”指标项中，可不考虑通用服务器的身份鉴别方式。	正确	错误		

3699	判断题	某三级信息系统，若采用密码模块安全等级为一级的智能密码钥匙（具有商用密码产品认证证书，且证书在有效期内）实现登录堡垒机时的身份鉴别，则智能密码钥匙符合GM/T 0115《信息系统密码应用测评要求》中对密码产品合规性的要求。	正确	错误		
3700	判断题	依据GM/T 0115《信息系统密码应用测评要求》，若堡垒机登录口令使用合规的SM3算法加密后传输，则堡垒机的身份鉴别可判定为符合。	正确	错误		
3701	判断题	依据GM/T 0115《信息系统密码应用测评要求》，某信息系统通过堡垒机对设备进行集中运维管理，管理员使用合规的智能密码钥匙登录堡垒机，采用基于国密算法的数字签名机制进行身份鉴别，若堡垒机服务端的验签未采用经商用密码检测认证合格的密码产品实现，则堡垒机的“身份鉴别”指标应判为部分符合。	正确	错误		
3702	判断题	依据GM/T 0115《信息系统密码应用测评要求》，经核查，某系统责任单位制定有被测系统的商用密码应用方案，则“建设运行”层面的“制定密码应用方案”测评指标则判定为符合。	正确	错误		
3703	判断题	某三级信息系统，在其密码应用方案中将设备和计算安全层面的“重要可执行程序完整性、重要可执行程序来源真实性”判定为不适用，且方案通过评估，则在测评过程中，依据GM/T 0115《信息系统密码应用测评要求》，可直接将该项判定为不适用。	正确	错误		

3704	判断题	依据GM/T 0115《信息系统密码应用测评要求》，应用和数据安全层面的测评对象应包含关键业务应用，具体参考经评估通过的密码应用方案设定的范围确定；如无密码应用方案,应根据网络安全等级保护定级报告描述的范围确定。	正确	错误		
3705	判断题	根据GM/T 0115《信息系统密码应用测评要求》，应用和数据安全层面的测评对象包括业务应用系统以及提供身份鉴别、完整性保护、机密性保护、不可否认性功能的密码产品。	正确	错误		
3706	判断题	依据GM/T 0115《信息系统密码应用测评要求》，对云平台的SAAS应用，应用和数据安全层面的测评由云平台负责，租户信息系统密评时可直接复用云平台测评结果。	正确	错误		
3707	判断题	被测业务应用系统采用基于角色的访问控制策略，用户通过角色配置获得该角色拥有的应用系统权限。依据GM/T 0115《信息系统密码应用测评要求》，应用和数据安全层面“访问控制信息完整性”测评实施主要核查应用系统用户角色配置信息、角色权限配置信息等是否采用了加解密或计算杂凑值等机制进行完整性保护。	正确	错误		
3708	判断题	经核查，被测业务应用系统无重要信息资源安全标记功能，则应用和数据安全层面“重要信息资源安全标记完整性”指标不适用。	正确	错误		

3709	判断题	依据GM/T 0115《信息系统密码应用测评要求》，应用和数据安全层面“重要数据传输机密性”的测评对象通常包括但不限于应用系统鉴别数据、重要业务数据、个人敏感信息、审计数据、日志数据、访问控制数据、重要配置数据等。	正确	错误		
3710	判断题	依据GM/T 0115《信息系统密码应用测评要求》，对于政务信息公开网站、门户网站等面向公众的业务应用系统，由于任何人均可访问，且网站数据可以公开，因此应用和数据安全层面“重要数据存储机密性”指标可判定为“不适用”。	正确	错误		
3711	判断题	依据GM/T 0115《信息系统密码应用测评要求》，在进行应用和数据安全层面“重要数据传输完整性”测评时，如果完整性保护采用的是数字签名技术，则测评人员可使用签名私钥对抓取的签名结果进行验证。	正确	错误		
3712	判断题	依据GM/T 0115《信息系统密码应用测评要求》，在进行应用和数据安全层面“重要数据存储完整性”指标测评时，如果现场条件不允许，可不对存储数据进行篡改测试。	正确	错误		
3713	判断题	经访谈和文档审查，某电子合同系统采用电子签章系统实现合同签署行为的不可否认性，在应用和数据安全层面“不可否认性”指标测评时，核查电子签章系统产品合规性和密码算法合规性即可。	正确	错误		

3714	判断题	根据GM/T 0115《信息系统密码应用测评要求》，在对第三/四级信息系统开展应急处置层面“应急策略”指标测评时，测评人员根据系统方提供的如下证据判定该测评指标为“符合”。证据为：被测单位提供的管理制度中具有密码应用应急策略文件，且应急策略中明确了密码应用安全事件监测预警机制、信息报送机制、应急处置措施、系统恢复流程、事件总结等内容。	正确	错误		
3715	判断题	在测评三级信息系统时，对于设备和计算安全层面“重要可执行程序完整性、重要可执行程序来源真实性”，可由信息系统责任方自行决定是否按照GM/T 0115《信息系统密码应用测评要求》进行测评和结果判定。	正确	错误		
3716	判断题	根据GM/T 0115《信息系统密码应用测评要求》，对于三级信息系统，在实施各技术安全层面的“访问控制信息完整性”指标测评时，密评人员应根据信息系统的密码应用方案和方案评估意见判定相应指标是否按照标准符合性测评。	正确	错误		
3717	判断题	根据GM/T 0115《信息系统密码应用测评要求》，对于“宜”的条款，存在两种“不适用”情形。	正确	错误		
3718	判断题	对于三级信息系统，在实施应用和数据安全层面的“不可否认性”指标测评时，若存在相应安全需求，则密评人员应按照GM/T 0115《信息系统密码应用测评要求》相应指标要求进行测评和结果判定。	正确	错误		

3719	判断题	根据某三级信息系统的密码应用需求，涉及到部分第四级信息系统密码应用的相关指标要求，那么在测评时只需要现场核实这些指标落实情况即可，无需将这些特殊情况的测评实施及结论体现在密码应用安全性评估报告中。	正确	错误		
3720	判断题	某三级信息系统，在测评应用和数据安全层面的“重要数据传输机密性”指标时，密评人员发现该系统部署了经检测认证合格的服务器密码机（安全等级二级）对重要数据进行加密保护，那么该测评单元的测评实施第二条可以直接判定为“符合”。	正确	错误		
3721	判断题	GM/T 0115《信息系统密码应用测评要求》中的风险分析和评价针对单元测评结果中产生的不符合项和部分符合项进行的。	正确	错误		
3722	判断题	依据GM/T 0115《信息系统密码应用测评要求》，在做密钥归档检查时，密评人员应重点核实归档密钥是否仅用于解密被加密的历史信息或验证被签名的历史信息。	正确	错误		
3723	判断题	依据GM/T 0115《信息系统密码应用测评要求》，对于三级信息系统，网络和通信安全层面“安全接入认证”指标，信息系统责任方可自行决定是否将其纳入标准符合性测评范围。	正确	错误		
3724	判断题	依据GM/T 0115《信息系统密码应用测评要求》，对于二级信息系统，物理和环境安全层面的测评对象仅涉及电子门禁系统。	正确	错误		

3725	判断题	经访谈，某电子门禁系统未采用密码技术来保证电子门禁系统进出记录数据的存储完整性，但记录数据每天都定时备份到数据库中，因此针对“电子门禁记录数据存储完整性”指标可以判定为部分符合。	正确	错误		
3726	判断题	在网络和通信安全层面的测评中发现，系统客户端通过互联网采用HTTPS协议访问应用系统，并使用用户名+口令的方式登录应用系统，因此可以认为是对通信实体进行了双向身份鉴别。	正确	错误		
3727	判断题	某三级信息系统运维用户通过互联网登录SSL VPN后，再通过堡垒机进行运维操作，如果SSL VPN具有商用密码产品认证证书，则可以认为运维管理终端到SSL VPN之间的通信信道是符合GM/T 0115《信息系统密码应用测评要求》的要求的。	正确	错误		
3728	判断题	依据GM/T 0115《信息系统密码应用测评要求》，针对网络和通信安全层面的“通信过程中重要数据的机密性”要求进行测评时，通过核查是否采用密码技术的加解密功能对通信过程中敏感信息或通信报文进行机密性保护，并验证敏感信息或通信报文机密性保护机制是否正确和有效，即可判定是否符合要求。	正确	错误		
3729	判断题	依据GM/T 0115《信息系统密码应用测评要求》，针对网络和通信安全层面的“安全接入认证”要求进行测评时，如条件允许，测评人员可尝试将未授权设备接入内部网络，核实即便非授权设备使用了合法IP地址，也无法访问内部网络。	正确	错误		

3730	判断题	依据GM/T 0115《信息系统密码应用测评要求》，进行安全管理制度测评时，应核查各项安全管理制度是否包括密码人员管理、密钥管理、建设运行、应急处置、设备软硬件及介质管理等制度。	正确	错误		
3731	判断题	某信息系统管理员在互联网通过合规的SSL VPN接入系统内网后登录堡垒机对通用服务器进行远程管理，SSL VPN建立合规的GMSSL通道并正确启用国密算法，则设备和计算安全层面“远程管理通道安全”测评单元可判定为“符合”。	正确	错误		
3732	判断题	密评人员对某二级信息系统进行测评时，经核实，系统中的设备仅进行本地运维，关闭了对外运维的接口。则该测评对象的“身份鉴别”、“远程管理通道安全”测评指标均可作为不适用项。	正确	错误		
3733	判断题	若管理员在互联网直接访问堡垒机（部署在机房中）对设备进行管理，在网络和通信安全层面将访问堡垒机的信息传输通道作为测评对象，在设备和计算安全层面则不能将该通道作为测评对象。	正确	错误		
3734	判断题	若管理员可在互联网直接访问堡垒机对设备进行管理，在网络和通信安全层面、设备和计算安全层面的“远程管理通道安全”测评单元均可将访问堡垒机的信息传输通道作为测评对象。	正确	错误		
3735	判断题	依据GM/T 0115《信息系统密码应用测评要求》，在设备和计算安全层面，具有商用密码产品认证证书的整机类密码产品，其“身份鉴别”、“日志记录完整性”测评指标可直接判定为符合。	正确	错误		

3736	判断题	依据GM/T 0115《信息系统密码应用测评要求》，在设备和计算安全层面，具有商用密码产品认证证书的整机类密码产品，且可以确定实际部署的密码产品与获认证产品一致的情况下，“系统资源访问控制信息完整性”、“重要可执行程序完整性、重要可执行程序来源真实性”，指标可判定为符合。	正确	错误		
3737	判断题	某三级信息系统在投入运行前进行了商用密码应用安全性评估，且具有相应的评估报告，则“投入运行前进行密码应用安全性评估”测评指标可判定为符合。	正确	错误		
3738	判断题	应用和数据安全层面测评时，经核查发现应用系统客户端调用智能密码钥匙对重要业务数据进行SM4加密和计算SM3杂凑值后传输，服务端调用服务器密码机进行SM4解密并校验SM3杂凑值，重要业务数据无其他传输场景，则可判定重要业务数据符合本层面“重要数据传输机密性”和“重要数据传输完整性”测评指标。	正确	错误		
3739	判断题	对于政务信息公开网站、门户网站等面向公众的业务应用系统，由于任何人均可访问，且网站数据可以公开，因此应用和数据安全层面的“身份鉴别”指标为“不适用”。	正确	错误		
3740	判断题	在对应用和数据安全层面“访问控制信息完整性”进行测评时，必须对生产环境下应用系统的权限、标签等配置信息进行篡改测试，才能验证完整性保护的有效性。	正确	错误		

3741	判断题	经访谈安全主管，被测三级信息系统投入运行以来尚未发生密码应用安全事件，则应急处置层面“事件处置”指标可直接判定为“不适用”。	正确	错误		
3742	判断题	某三级信息系统在网络和通信安全层面，虽然存在通信实体的双向身份鉴别安全需求，但由于标准条款中对三级系统并未强制要求必须双向鉴别，所以在实际测评时，依据GM/T 0115《信息系统密码应用测评要求》仅核查单向鉴别即可。	正确	错误		
3743	判断题	在车联网场景下，智能网联汽车接入运营商网络时，会对汽车身份的真实性进行确认，具体采用经商用密码认证合格的密码产品提供的SM2数字签名技术实现，则网络和通信安全层面“身份鉴别”指标可判定为“符合”。	正确	错误		
3744	判断题	某单位总公司和分公司在不同城市，双方网络层通信仅采用HTTP协议，但是应用和数据安全层面的“重要数据传输机密性”是符合的，那么对于网络和通信安全层面“通信过程中重要数据的机密性”测评指标可直接判定为“部分符合”且存在“高风险”。	正确	错误		
3745	判断题	对于使用满足GM/T 0036并获得商用密码产品认证证书的电子门禁系统，物理和环境安全层面的“身份鉴别”、“电子门禁记录数据存储完整性”可以复用密码产品检测认证结果。	正确	错误		

3746	判断题	测评人员在对某三级信息系统的网络和通信安全层面抓包分析时发现，通信过程中IPSec协议通信双方均发送其签名证书和加密证书，双证书分别用于身份鉴别和会话加密。	正确	错误		
3747	判断题	根据GM/T 0115《信息系统密码应用测评要求》，对于三级信息系统，密钥管理员、密码安全审计员、密码操作员应由本机构的内部员工担任，并必须在任前对其进行背景调查。	正确	错误		
3748	判断题	根据GM/T 0115《信息系统密码应用测评要求》，当密码应用安全管理制度和操作规程在执行过程中发现存在问题时，可以随时进行修订，替换掉存在问题的部分，无需再次评审。	正确	错误		
3749	判断题	在某三级系统的测评中发现，被测单位在制度中规定了人员离岗时及时终止其所有密码应用相关的访问权限、操作权限，并具有相关的记录。因此“建立关键岗位人员保密制度和调离制度”指标的判定结果可判定为“符合”。	正确	错误		
3750	判断题	密评人员在对网络和通信安全层面进行测评时，可通过端口扫描工具探测IPSec VPN和SSL VPN服务端所对应的端口服务是否开启，其中SSL VPN服务要求开启TCP 443端口，不得修改端口。	正确	错误		

3751	判断题	根据GM/T 0115《信息系统密码应用测评要求》，在测评设备和计算安全层面时，针对系统类的密码产品（如电子签章系统、数字证书认证系统），若密码产品具有合格的商用密码产品认证证书，则该密码产品的“系统资源访问控制信息完整性”测评指标可直接判定为符合。	正确	错误		
3752	判断题	根据GM/T 0115《信息系统密码应用测评要求》，若系统通过调用合规的服务器密码机，使用SM3算法（加盐值）计算设备日志记录的杂凑值并定期进行校验，则能够实现设备日志记录的完整性保护。	正确	错误		
3753	判断题	根据GM/T 0115《信息系统密码应用测评要求》，某三级信息系统重要可执行程序在生成时基于数字签名技术进行签名，在应用服务器端调用时未做验签，数字签名计算使用的密码算法、密码产品和密钥管理等均合规，则针对“设备和计算安全”层面的“重要可执行程序完整性、重要可执行程序来源真实性”测评指标的判定结果为“部分符合”。	正确	错误		
3754	判断题	根据GM/T 0115《信息系统密码应用测评要求》，管理员在互联网通过SSL VPN接入系统内网，由于SSL VPN建立了网络和通信安全层面的通信信道，故SSL VPN不作为“设备和计算安全层面”的测评对象。	正确	错误		
3755	判断题	某信息系统密码应用方案中写明设备和计算安全层面未设置重要信息资源安全标记，明确“重要信息资源安全标记”为不适用项，且密码应用方案通过评估，测评人员经核查系统满足方案中的不适用理由，因此该指标可判定为“不适用”。	正确	错误		

3756	判断题	管理员在互联网通过合规的SSL VPN接入系统内网，管理员使用合规的智能密码钥匙登录SSL VPN，并正确启用国密算法，则“网络和通信安全”层面的“身份鉴别”指标可直接判定为符合。	正确	错误		
3757	判断题	某三级信息系统管理员使用智能密码钥匙（经过商用密码检测认证且符合相应的密码模块安全等级）登录堡垒机，其中智能密码钥匙长期插入在访问堡垒机的客户端上，用户通过浏览器输入堡垒机访问地址后可直接访问，则针对设备和计算安全层面的堡垒机“身份鉴别”指标测评结果为“部分符合”。	正确	错误		
3758	判断题	对于信息系统中部署和使用的密码设备，核查其商用密码产品认证证书时发现其证书已过期，则认定该密码设备一定不符合GM/T 0115《信息系统密码应用测评要求》中对“密码产品合规性”的要求。	正确	错误		
3759	判断题	某云管平台面向云管理员提供云资源统一调度、统一管理等功能，面向云租户提供资源实例的申请开通、资源实例的操作等功能。在对该云管平台进行应用和数据安全层面“身份鉴别”指标测评时，只需要核查云管理员用户的身份鉴别机制，云租户用户的身份鉴别机制应在云租户信息系统密评时核实。	正确	错误		

3760	判断题	某行业主管部门建设电子认证服务系统为本行业提供数字证书制作及签发服务，其网络安全等级保护定级为三级。该系统主要业务应用为数字证书认证系统应用，经核查，应用各类用户登录可采用智能密码钥匙基于SM2数字签名技术进行身份鉴别，且均同时支持用户名+口令的方式登录以防止智能密码钥匙鉴别失效导致业务中断；其中数字证书认证系统已经商用密码认证机构认证合格。依据GM/T 0115《信息系统密码应用测评要求》，该系统应用和数据安全层面的“身份鉴别”单元测评结果为“部分符合”。	正确	错误		
3761	判断题	在对应用和数据安全层面“身份鉴别”指标测评时发现，应用系统业务用户采用了具有商用密码产品认证证书（证书在有效期内）的智能密码钥匙进行用户登录身份鉴别，具体为智能密码钥匙与用户身份ID绑定，应用通过读取智能密码钥匙中存储的用户ID做身份鉴别，则针对应用用户“身份鉴别”指标的测评结果至少为“部分符合”。	正确	错误		
3762	判断题	政务云平台部署密码支撑平台提供密码资源的统一调度，密码支撑平台采用token验证的方式对接入的租户业务应用系统进行鉴权，该过程可考虑在应用和数据安全层面进行“身份鉴别”指标测评。	正确	错误		

3763	判断题	在对应用和数据安全层面“重要数据传输机密性”指标测评时，经使用协议分析工具捕获并分析某系统重要业务数据传输过程中的数据包，发现重要业务数据先进行BASE64编码再使用SHA256杂凑后传输，则针对“重要数据传输机密性”指标的测评结果至少为“部分符合”。	正确	错误		
3764	判断题	经核查发现某被测业务应用通过调用服务器密码机采用SM4-GCM实现姓名、手机号、身份证号等重要用户信息存储完整性保护，服务器密码机及其密码模块安全等级合规，数据库中数据格式符合预期，则该测评对象的“重要数据存储完整性”指标可判定为符合。	正确	错误		
3765	判断题	某WEB应用系统采用HTTPS协议保障重要数据传输的机密性和完整性，经使用协议分析工具捕获并分析Server Hello消息数据包，密码套件为TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA384，则被测对象部分符合“应用和数据安全”层面的“重要数据传输机密性”和“重要数据传输完整性”测评指标。	正确	错误		
3766	判断题	某二级信息系统业务应用具有“不可否认性”安全需求，并由部署的电子签章系统提供相关功能，由于GM/T 0115《信息系统密码应用测评要求》中未给出第二级信息系统应用和数据安全层面“不可否认性”指标的测评要求，因此该电子签章系统及其实现功能等无法纳入测评范围。	正确	错误		

3767	判断题	根据GM/T 0115《信息系统密码应用测评要求》，应用系统采用静态口令对登录用户进行身份鉴别，口令信息采用合规的密码技术进行加密传输，且采用单向递增函数实现鉴别信息防重用，则应用和数据安全层面“身份鉴别”单元测评结果有可能为符合。	正确	错误		
3768	判断题	对某三级信息系统的通信信道进行测评时，发现通信实体身份鉴别使用的数字证书的签名算法标识为“1.2.156.10197.1.501”，则可直接判定“身份鉴别”测评指标为“符合。	正确	错误		
3769	单项选择题	根据GM/T 0116《信息系统密码应用测评过程指南》，以下关于测评方对信息系统开展密码应用安全性评估时，应遵循的原则，其中错误的是（ ）。	可重复性和可再现性原则	经济性原则	客观公正性原则	结果完善性原则
3770	单项选择题	根据GM/T 0116《信息系统密码应用测评过程指南》，以下关于测评工作中可能面临的风险，正确的是（ ）。	验证测试可能影响被测信息系统正常运行	工具测试可能影响被测信息系统正常运行	可能导致被测信息系统敏感信息泄露	以上都是
3771	单项选择题	根据GM/T 0116《信息系统密码应用测评过程指南》，以下哪种情形不属于测评风险（ ）。	验证系统功能时产生了冗余数据	上机查看配置时获取了重要设备的身份鉴别信息	对委托方搭建的测试系统进行了攻击测试	测试过程中产生了较大网络流量影响了系统的负载
3772	单项选择题	根据GM/T 0116《信息系统密码应用测评过程指南》，以下测评风险规避措施，错误的是（ ）。	签署保密协议	将无法直接接入测试工具采集相关数据的测试对象从测试范围中去除	签署测试授权书	工具测试避开业务运行高峰期
3773	单项选择题	根据GM/T 0116《信息系统密码应用测评过程指南》，以下关于现场测评过程中的测评风险规避措施，错误的是（ ）。	需进行验证测试和工具测试时，应避开被测信息系统业务高峰期	需进行验证测试和工具测试时，可以配置与被测信息系统一致的模拟/仿真环境开展测评工作	需进行上机验证测试时，密评人员需要在已授权的情况下进行实际验证操作	整个现场测评过程，需要由被测单位和测评方相关人员进行监督。

3774	单项选择题	根据GM/T 0116《信息系统密码应用测评过程指南》，以下哪项内容不属于测评准备活动的主要任务（ ）。	项目启动	信息收集和分析	签署风险确认书	工具和表单准备
3775	单项选择题	根据GM/T 0116《信息系统密码应用测评过程指南》，测评准备活动中与项目相关的主要文档是（ ）。	项目管理计划	项目计划书	测评指导书	任务书
3776	单项选择题	根据GM/T 0116《信息系统密码应用测评过程指南》，校准本次测评过程中可能用到的测评工具，发生在（ ）测评活动中。	测评准备活动	方案编制活动	现场测评活动	分析与报告编制活动
3777	单项选择题	根据GM/T 0116《信息系统密码应用测评过程指南》，以下哪项不属于测评准备活动的输出文档（ ）。	系统情况调研表	签署过的测评授权书	选用的测评工具清单	会议签到表
3778	单项选择题	根据GM/T 0116《信息系统密码应用测评过程指南》，以下关于测评准备活动的输出文档及其内容，说法正确的是（ ）。	调查表格、被测信息系统相关的技术资料内容应涵盖被测信息系统的网络安全保护等级、业务情况、软硬件情况、密码应用情况、密码管理情况	工具和表单准备阶段输出物的内容应涵盖测评工具、现场测评授权、测评可能带来的风险、交接的文档名称、会议记录表单、会议签到表单等	项目计划书至少应涵盖项目概述、工作依据、技术思路、工作内容和项目组织等内容。	以上内容均正确
3779	单项选择题	根据GM/T 0116《信息系统密码应用测评过程指南》，密码应用安全性评估活动中，确定测评对象和测评指标是在（ ）阶段。	测评准备活动	方案编制活动	现场测评活动	分析与报告编制活动
3780	单项选择题	根据GM/T 0116《信息系统密码应用测评过程指南》，在密评工作方案编制活动中，关于被测信息系统的核心资产确定，以下说法不正确的是（ ）。	核心资产及其他需要保护的配套数据、敏感安全参数的威胁模型和安全策略等均由被测单位自主确定。	测评方需要多对信息系统的核心资产进行核查和确认。	核心资产可以是业务应用、业务数据或者业务应用的某些设备、组件。	被测单位需要确定被测信息系统需要保护的核心资产，以及相应的威胁模型和安全策略。

3781	单项选择题	根据GM/T 0116《信息系统密码应用测评过程指南》，以下不是被测信息系统密评工作中对硬件设备进行描述的内容的是（ ）。	测评对象所属区域	测评对象设备名称	测评对象设备信息	测评对象数据加密情况
3782	单项选择题	根据GM/T 0116《信息系统密码应用测评过程指南》，在确定测评的不适用项时，如无密码应用方案，以下哪项不作为不适用项的论证依据（ ）。	是否在被测系统责任边界内	系统安全需求	不适用的具体原因	是否采用了可满足安全要求的其他替代性风险控制措施
3783	单项选择题	根据GM/T 0116《信息系统密码应用测评过程指南》，测评指标的确定需要依据（ ）。	调查表格	GM/T 0115《信息系统密码应用测评要求》	通过评估的密码应用方案	以上均包括
3784	单项选择题	根据GM/T 0116《信息系统密码应用测评过程指南》，测评检查点确定时，应充分考虑到（ ）。	密码产品是否正确配置	检查的可行性和风险，对被测信息系统的影响	承载核心资产流转的设备	系统采用的密码服务情况
3785	单项选择题	根据GM/T 0116《信息系统密码应用测评过程指南》，以下关于测评工具接入点的选择，错误的是（ ）。	信息系统测评工具接入点需要选择三个或三个以上。	从系统内部同一网段接入时，测试工具一般接在与被测对象在同一网段的交换机上	当从被测信息系统边界外接入时，测试工具一般接在系统边界设备上	从系统内部不同网段接入时，测试工具一般接在与被测对象不在同一网段的内部核心交换机上
3786	单项选择题	根据GM/T 0116《信息系统密码应用测评过程指南》，以下不属于测评方案主要内容的是（ ）。	测评对象	测评指标	测评检查点	风险评估结果
3787	单项选择题	根据GM/T 0116《信息系统密码应用测评过程指南》，以下不是现场测评活动工作的三项主要内容的是（ ）。	现场测评准备	现场测评和结果记录	测评内容签字确认	结果确认和资料归还
3788	单项选择题	根据GM/T 0116《信息系统密码应用测评过程指南》，现场测评活动不包含下列哪一项（ ）。	确认整体密码部署是否合规	实地检查密码配置是否正确	测评检查点的确定	授权接入系统后确认密码使用是否有效

3789	单项选择题	根据GM/T 0116《信息系统密码应用测评过程指南》，关于采集分析被测信息系统与外界通信的数据以及被测信息系统内部传输和存储的数据，以下说法不正确的是（ ）。	应分析使用的密码算法、密码协议、关键数据结构是否合规	应检查传输的口令、用户隐私数据等重要数据是否进行了保护	应验证杂凑值和签名值是否正确	通过加解密等方式进行对称加密算法的验证
3790	单项选择题	根据GM/T 0116《信息系统密码应用测评过程指南》，以下关于测评过程中被测系统数据安全保护措施验证、数据采集方法说明，说法错误的是（ ）。	在条件允许的情况下，可以重放采集的关键数据（如身份鉴别数据）验证被测信息系统是否具备防重放攻击的能力	在条件允许的情况下，可以尝试修改传输的数据验证被测信息系统是否对传输数据进行了完整性保护	如果被测系统无法提供数据接入条件，可以不进行数据采集。	在条件允许的情况下，可以搭建与被测信息系统一致的模拟/仿真环境开展测评工作
3791	单项选择题	根据GM/T 0116《信息系统密码应用测评过程指南》，密评人员在对关键设备进行现场检查时，测评工具接入被测信息系统条件不成熟，测评方应（ ）。	自行模拟被测信息系统搭建测评环境获取测评数据	与被测单位协商、配合，生成必要的离线数据	告知被测单位风险后，接入被测系统获取真实数据	将该测评项做不适用处理
3792	单项选择题	根据GM/T 0116《信息系统密码应用测评过程指南》，以下关于密评工作中结果确认和资料归还部分描述不正确的是（ ）。	密评人员在现场测评完成后，应首先汇总现场测评的测评记录，对遗漏和需要进一步验证的内容实施补充测评	召开测评现场结束会，对测评过程中得到各类测评结果记录进行现场沟通和确认	现场测评活动结束后，可以保留现场测评材料至评估报告编写完成	归还测评过程中借阅的所有文档资料，将测评现场环境恢复至测评前状态
3793	单项选择题	根据GM/T 0116《信息系统密码应用测评过程指南》，以下关于现场测评活动的输出文档，描述正确的是（ ）。	现场测评准备阶段输出文档包括会议记录、更新确认后的密评方案、确认的测评授权书和风险告知书等	现场测评和结果记录阶段输出文档主要为各类测评结果记录	测评结果确认和资料 归还阶段的输出文档为经过被测单位确认的各类测评结果记录	以上内容均正确

3794	单项选择题	根据GM/T 0116《信息系统密码应用测评过程指南》，以下哪个不属于现场测评活动的输出文档（ ）。	更新确认的密评方案	各类测评结果记录	签署过的测评授权书	项目计划书
3795	单项选择题	根据GM/T 0116《信息系统密码应用测评过程指南》，以下关于分析与报告编制活动的输入文档，不正确的是（ ）。	单元测评：经过被测单位确认的各类测评结果记录、GM/T 0115	密评报告编制：经过评审和确认的密评报告	量化评估：密评报告的单元测评的结果汇总及整体测评部分	风险分析：完成的调查表格，密评报告的整体测评结果和量化评估部分，相关风险评估标准
3796	单项选择题	根据GM/T 0116《信息系统密码应用测评过程指南》，以下不属于分析与报告编制活动的主要任务的是（ ）。	单元测评	整体测评	风险分析	评估结论修正
3797	单项选择题	根据GM/T 0116《信息系统密码应用测评过程指南》，以下哪项不属于分析与报告编制活动（ ）。	威胁分析	量化评估	整体测评	风险分析
3798	单项选择题	根据GM/T 0116《信息系统密码应用测评过程指南》，单元测评阶段需要密评人员针对各测评单元涉及的各个测评对象，将实际获得的多个测评结果与（ ）相比较，分别判断每个测评结果与预期结果之间的符合性，综合判定该测评对象的测评结果，从而得到每个测评对象对应的测评结果。	测评对象	实际配置	访谈内容	预期结果
3799	单项选择题	根据GM/T 0116《信息系统密码应用测评过程指南》，以下关于量化评估的说法，不正确的是（ ）。	量化评估的输入是密评报告的单元测评的结果汇总及整体测评部分	根据单元测评结果，计算各测评指标的各个测评对象的测评结果符合程度得分，之后再进行整体测评	根据各个测评对象的符合程度得分，计算各测评单元得分	根据各测评单元、各层面和整体得分，总体评价被测信息系统已采取的有效保护措施和存在的密码应用安全问题情况。

3800	单项选择题	根据GM/T 0116《信息系统密码应用测评过程指南》，根据威胁类型和威胁发生频率，判断测评结果汇总中（ ）所产生的安全问题被威胁利用的可能性，可能性的取值范围为高、中和低。	部分符合项	不符合项	部分符合项或不符合项	符合项、部分符合项和不符合项
3801	单项选择题	根据GM/T 0116《信息系统密码应用测评过程指南》，风险分析的输入不包括（ ）。	被测系统威胁分析结果	被测系统的规模	被测系统存在的安全问题	已有安全措施情况
3802	单项选择题	根据GM/T 0116《信息系统密码应用测评过程指南》，以下关于密评报告编制过程的说法，错误的是（ ）。	密评报告通过内部评审后，由授权签字人进行签发，提交被测单位。	根据被测单位要求，多个定级的信息系统可合并形成一份报告	针对被测信息系统存在的安全问题，提出相应改进建议，并编制密评报告安全文件及改进建议部分	密评报告编制完成后，测评方应根据委托测评协议书、被测单位提交的相关文档、测评原始记录和其他辅助信息，对密评报告进行内部评审
3803	单项选择题	根据GM/T 0116《信息系统密码应用测评过程指南》，以下关于密评报告编制工作，描述错误的是（ ）。	密评人员整理各项任务输出，编制密评报告相应部分。对每一个定级的被测信息系统应单独形成一份密评报告。	针对被测信息系统存在的安全问题，提出相应改进建议，并编制密评报告改进建议部分。	密评报告编制完成后，测评方应根据委托测评协议书、被测单位提交的相关文档、测评原始记录和其他辅助信息，将密评报告提交委托单位进行评审。	密评报告通过内部评审或专家评审后，由授权签字人进行签发，提交被测单位。

3804	单项选择题	根据GM/T 0116《信息系统密码应用测评过程指南》，以下关于分析与报告编制活动的输出文档及其内容描述错误的是（ ）。	单元测评文档内容：汇总统计各测评指标的各个测评对象的测评结果，给出单元测评结果	量化评估文档内容：综合单元测评和整体测评结果，计算得分，并对被测信息系统的密码应用情况安全性进行总体评价	风险分析文档内容：分析被测信息系统整体安全状况及对各测评对象测评结果的修正情况	密评报告编制文档内容：测评项目概述、被测系统情况、测评范围与方法、整体测评、量化评估、评估结论、安全问题及改进建议等
3805	单项选择题	根据《关于规范商用密码应用安全性评估结果备案工作的通知》（国密局字〔2021〕392号），运营者在完成商用密码应用安全性评估工作后，应在（ ）日内将评估结果报密码管理部门备案。	10	15	20	30
3806	多项选择题	根据GM/T 0116《信息系统密码应用测评过程指南》，以下哪项任务是方案编制活动中的主要任务（ ）。	测评人员确定	测评对象确定	测评指标确定	测评检查点确定
3807	多项选择题	根据GM/T 0116《信息系统密码应用测评过程指南》，以下关于测评方对信息系统开展密码应用安全性评估时，应遵循的原则，正确的是（ ）。	可重复性和可再现性原则	可重用性原则	客观公正性原则	结果完善性原则
3808	多项选择题	根据GM/T 0116《信息系统密码应用测评过程指南》，在对信息系统开展密码应用安全性评估时，以下属于测评实施过程中客观公正性原则的是（ ）。	测评方应保证在符合国家密码管理部门要求及最佳主观判断情形	测评方案需要测评方与被测单位共同认可	测评过程需要基于明确定义的测评方式和解释	方案合理，测评方即可开展现场测评活动
3809	多项选择题	根据GM/T 0116《信息系统密码应用测评过程指南》，测评方对信息系统开展密码应用安全性评估时，应遵循的原则，正确的是（ ）。	测评方应保证在符合国家密码管理部门要求及最小主观判断情形	测评工作可重用商用密码检测认证结果	测评工作可重用密码应用安全性评估的测评结果	测评所产生的结果应客观反映信息系统的密码应用现状

3810	多项选择题	根据GM/T 0116《信息系统密码应用测评过程指南》，以下关于可重复性和可再现性原则正确的是（ ）。	按照同样的要求，不同的密评人员对每个测评实施过程的重复执行应得到同样的结果	在同样的环境下，不同的密评人员对每个测评实施过程的重复执行应得到同样的结果	可再现性关注不同密评人员测评结果的一致性	可重复性关注同一密评人员测评结果的一致性
3811	多项选择题	根据GM/T 0116《信息系统密码应用测评过程指南》，测评方对信息系统开展密码应用安全性评估时，应遵循的原则，错误的是（ ）。	测评工作可重用密码应用安全性评估的测评结果	测评方应保证在符合国家密码管理部门要求及最佳主观判断情形	方案合理，测评方即可开展现场测评活动	测评所产生的结果应客观反映信息系统的密码应用现状
3812	多项选择题	根据GM/T 0116《信息系统密码应用测评过程指南》，以下哪些情形属于测评风险（ ）。	验证系统功能时产生了冗余数据	上机查看配置时获取了重要设备的身份鉴别信息	对委托方搭建的测试系统进行了攻击测试	测试过程中产生了较大网络流量影响了系统的负载
3813	多项选择题	根据GM/T 0116《信息系统密码应用测评过程指南》，在被测系统测评过程中，测评工作面临的风险主要包括（ ）。	人员访谈可能影响系统正常运维工作	验证测试可能影响被测信息系统正常运行	工具测试可能影响被测信息系统正常运行	可能导致被测信息系统敏感信息泄露
3814	多项选择题	根据GM/T 0116《信息系统密码应用测评过程指南》，以下哪些风险规避措施有效（ ）。	签署保密协议	将无法直接接入测试工具采集相关数据的测试对象从测试范围中去除	签署测试授权书	工具测试避开业务运行高峰期
3815	多项选择题	根据GM/T 0116《信息系统密码应用测评过程指南》，以下测评风险规避措施不正确的是（ ）。	双方签署委托测评协议书明确测评的目标、范围、计划等	双方签署保密协议	在业务高峰期进行压力测试以充分验证系统安全措施的有效性	需进行上机验证测试时，由密评人员自行进行实际操作
3816	多项选择题	根据GM/T 0116《信息系统密码应用测评过程指南》，以下关于测评过程包括四项基本测评活动，描述正确的是（ ）。	测评准备活动包括项目启动、信息收集和分析等	方案编制活动包括测评检查点确定、测评内容确定等	现场测评活动包括现场测评和结果记录、结果确认和资料归还等	分析与报告编制活动包括单元测评、整体测评、风险分析等
3817	多项选择题	根据GM/T 0116《信息系统密码应用测评过程指南》，项目计划书应包含（ ）等内容。	项目概述、工作依据说明	技术思路	不适用指标描述	工作内容和项目组织安排

3818	多项选择题	根据GM/T 0116《信息系统密码应用测评过程指南》，在测评准备阶段进行是信息收集和分析的过程中，测评方可以使用（　）等方式，了解被测信息系统的构成和密码应用情况，为编写密评方案和开展现场测评工作奠定基础。	填写调查表格	查阅资料	现场调查	预测试
3819	多项选择题	根据GM/T 0116《信息系统密码应用测评过程指南》，在测评准备阶段进行是信息收集和分析的过程中，测评方收集测评所需资料包括（ ）。	被测信息系统总体描述文件、密码应用总体描述文件	网络安全等级保护定级报告、网络安全等级保护测评报告	安全总体方案、安全详细设计方案、密码应用方案	密码产品的用户操作指南、密码应用安全规章制度
3820	多项选择题	根据GM/T 0116《信息系统密码应用测评过程指南》，以下哪些材料为测评方需要收集的（ ）。	被测信息系统总体描述文件	被测信息系统密码应用总体描述文件	被测系统密码应用方案	等级保护定级报告及等级测评报告
3821	多项选择题	根据GM/T 0116《信息系统密码应用测评过程指南》，在测评准备阶段工具和表单准备活动中，需要项目组提前准备并打印的表单包括（ ）。	合同文件	现场测评授权书	风险告知书、文档交接单	会议记录表单、会议签到表单等。
3822	多项选择题	根据GM/T 0116《信息系统密码应用测评过程指南》，下列文档属于测评准备活动阶段需要输出的是（ ）。	现场测评授权书	密评方案	项目计划书	会议签到表单
3823	多项选择题	根据GM/T 0116《信息系统密码应用测评过程指南》，以下关于测评准备活动的输出文档及其内容，说法正确的是（ ）。	在项目启动任务中，输入文档包括委托测评协议书、保密协议等，输出文档为项目计划书	在信息收集和分析任务中，输入文档为调查表格，输出文档为调查表格、被测信息系统相关的技术资料	在工具和表单准备任务中输出文档为选用的测评工具清单，打印的各类表单。	调查表格、被测信息系统相关的技术资料内容应涵盖被测信息系统的网络安全保护等级、业务情况、软硬件情况、密码应用情况、密码管理情况等
3824	多项选择题	根据GM/T 0116《信息系统密码应用测评过程指南》，以下属于测评准备活动的输出文档的是（ ）。	系统情况调研表	签署的合同	选用的测评工具清单	会议签到表

3825	多项选择题	根据GM/T 0116《信息系统密码应用测评过程指南》，在密码应用安全性评估过程中，以下哪些属于测评准备阶段的活动（ ）。	项目启动	现场测评	信息收集和分析	工具和表单准备
3826	多项选择题	根据GM/T 0116《信息系统密码应用测评过程指南》，以下哪些不是测评方案编制活动的主要任务（ ）。	现场测评准备	单项测评结果判定	测评检查点确定	确认测评工具的可用性
3827	多项选择题	根据GM/T 0116《信息系统密码应用测评过程指南》，在密评工作方案编制活动中，测评对象确定阶段的主要任务包括（ ）。	识别被测信息系统的基本情况	描述被测信息系统	确定测评对象、描述测评对象	资产和威胁评估
3828	多项选择题	根据GM/T 0116《信息系统密码应用测评过程指南》，以下关于测评方案编制活动中，测评对象确定阶段的任务描述，正确的是（ ）。	描述被测信息系统时，一般以被测信息系统的网络拓扑结构为基础，采用总分式的描述方法	被测单位需要确定被测信息系统需要保护的核心资产，以及相应的威胁模型和安全策略	资产的价值根据资产的重要性和关键程度确定	核心资产及其他需要保护的配套数据、敏感安全参数的威胁模型和安全策略等均由被测单位根据密码应用方案、网络安全等级保护定级报告等确定，并由测评方进行核查和确认
3829	多项选择题	根据GM/T 0116《信息系统密码应用测评过程指南》，资产的价值根据资产的（ ）确定。	资产的可用性	资产的重要性	资产的价格	资产的关键程度
3830	多项选择题	根据GM/T 0116《信息系统密码应用测评过程指南》，测评指标确认的依据包括（ ）。	被测信息系统的定级结果	信息系统密码应用测评要求	相关行业标准及规范	密码应用方案

3831	多项选择题	根据GM/T 0116《信息系统密码应用测评过程指南》，测评检查点确定的主要内容有（ ）。	列出需要接受现场检查的关键设备和检查内容	确定测试路径和工具接入点，采用图示的方式描述测评工具的接入点、测试目的、测试途径和测试对象等相关内容	确定选用的测评工具，并进行校准	不适用测评指标分析
3832	多项选择题	根据GM/T 0116《信息系统密码应用测评过程指南》，实施密码应用管理要求评估时，以下哪些选项属于可能的测评对象（ ）。	安全管理制度	加密机操作操作规程	系统密码应用方案	安全事件记录
3833	多项选择题	根据GM/T 0116《信息系统密码应用测评过程指南》，密评方案应包括以下内容（ ）。	项目概述	测评对象、测评指标	测评检查点	单元测评实施
3834	多项选择题	根据GM/T 0116《信息系统密码应用测评过程指南》，以下关于密评方案编制过程中任务描述正确的是（ ）。	根据委托测评协议书和完成的调查表格，提取项目来源、被测单位整体信息化建设情况及被测信息系统与其他系统之间的连接情况等。	结合被测信息系统的实际情况，根据通过评估的密码应用方案及GM/T 0115，明确测评活动所要依据和参考的与密码算法、密码技术、密码产品和密码服务相关的标准规范。	依据委托测评协议书和被测信息系统的情况，估算现场测评工作量。	根据测评项目组成员分工，编制工作安排。
3835	多项选择题	根据GM/T 0116《信息系统密码应用测评过程指南》，以下关于测评方案编制活动的输出文档及文档内容，说法正确的是（ ）。	输出文档包含测评对象部分、测评指标部分、测评实施部分等内容	测评指标部分应说明被测信息系统相应等级对应的适用和不适用的测评指标	测评工作所需的人员、资料、场所等保障要求需要在客户确认测评方案后单独进行沟通确认。	密评方案应包括但不限于以下内容：项目概述、测评对象、测评指标、测评检查点以及单元测评实施等。

3836	多项选择题	根据GM/T 0116《信息系统密码应用测评过程指南》，以下哪项属于现场测评活动的内容（ ）。	召开首次会	与委托方确认测评记录	形成单元测评结果	传输数据采集分析
3837	多项选择题	根据GM/T 0116《信息系统密码应用测评过程指南》，密码应用安全性评估活动过程中，（ ）属于现场测评阶段的活动。	现场测评和结果记录	现场测评准备	结果确认和资料归还	单项测评结果判定
3838	多项选择题	根据GM/T 0116《信息系统密码应用测评过程指南》，现场测评活动包含下列哪几项（ ）。	确认整体密码部署是否合规	实地检查密码配置是否正确	测评检查点的确定	授权接入系统后确认密码使用是否有效
3839	多项选择题	根据GM/T 0116《信息系统密码应用测评过程指南》，采集分析被测信息系统与外界通信的数据以及被测信息系统内部传输和存储的数据时，需从以下方面进行（ ）。	分析使用的密码算法、密码协议、关键数据结构是否合规	检查传输的口令、用户隐私数据等重要数据是否进行了保护	验证杂凑值和签名值是否正确	条件允许的情况下可模拟进行重放攻击
3840	多项选择题	根据GM/T 0116《信息系统密码应用测评过程指南》，以下关于针对已经取得商用密码产品认证证书的密码产品的测评工作，说法正确的是（ ）。	需要针对密码产品依据产品或检测标准指标进行逐条判定并记录测评结果	无需其本身进行重复检测，主要进行符合性核验和配置检查	可以联系密码产品审批部门或相应的检测认证机构进行确认	无需针对设备进行检测，所有测评内容均可判定为符合
3841	多项选择题	根据GM/T 0116《信息系统密码应用测评过程指南》，以下关于测评过程中数据采集和分析工作，说法正确的是（ ）。	需要检查传输的口令、用户隐私数据等重要数据是否进行了保护（如对密文进行随机性检测、查看关键字段是否以明文出现），验证杂凑值和签名值是否正确	需要重点采集被测信息系统与外界通信的数据以及被测信息系统内部传输和存储的数据，分析使用的密码算法、密码协议、关键数据结构（如数字证书格式）是否合规	在条件允许的情况下，可以重放采集的关键数据（如身份鉴别数据）验证被测信息系统是否具备防重放攻击的能力	在条件允许的情况下，可以尝试修改存储的数据验证被测信息系统是否对存储数据进行了完整性保护

3842	多项选择题	根据GM/T 0116《信息系统密码应用测评过程指南》，为了验证密码产品是否被正确、有效地使用，可采集密码产品和其调用者之间的通信数据，通过采集的（ ），分析密码产品的调用是否符合预期。	密码产品的配置文件	密码产品调用指令	密码产品响应报文	密码产品的日志记录
3843	多项选择题	根据GM/T 0116《信息系统密码应用测评过程指南》，密评人员在对关键设备进行现场检查时，若测评工具接入被测信息系统条件不成熟时。以下测评操作，不正确的是（ ）。	自行模拟被测信息系统搭建测评环境获取测评数据	与被测单位协商、配合，生成必要的离线数据	告知被测单位风险后，接入被测系统获取真实数据	将该测评项做不适用处理
3844	多项选择题	根据GM/T 0116《信息系统密码应用测评过程指南》，以下哪些属于现场测评活动的输出文档（ ）。	更新确认的密评方案	各类测评结果记录	签署过的测评授权书	风险告知书
3845	多项选择题	根据GM/T 0116《信息系统密码应用测评过程指南》，单元测评主要是针对各测评指标中的各个测评对象，客观、准确地分析测评证据，对每个测评对象分别进行（ ）。	记录修改	测评实施	结果判定	综合分析
3846	多项选择题	根据GM/T 0116《信息系统密码应用测评过程指南》，以下关于测评单元结果判定正确的是（ ）。	测评单元包含的所有测评对象的测评结果均为符合或部分符合，则对应测评单元结果判定为符合。	测评单元包含的所有测评对象的测评结果均为不符合，则对应测评单元结果判定为不符合。	测评单元包含的所有测评对象的测评结果均为不适用，则对应测评单元结果判定为不适用。	测评单元包含的所有测评对象的测评结果不全为符合或不符合，则对应测评单元结果判定为部分符合。
3847	多项选择题	根据GM/T 0116《信息系统密码应用测评过程指南》，每个测评对象对应的测评结果可能是（ ）。	符合	不符合	部分符合	不适用
3848	多项选择题	根据GM/T 0116《信息系统密码应用测评过程指南》，关于整体测评，以下说法错误的是（ ）。	整体测评的输出是密评报告的单元测评结果修正部分	整体测评是对各个单元测评结果进行汇总分析，统计符合情况	整体测评包括测评单元间的整体测评、层面间的整体测评	测评单元的量化评估在整体测评前完成

3849	多项选择题	根据GM/T 0116《信息系统密码应用测评过程指南》，整体测评任务针对测评结果为（　）的测评对象，采取逐条判定的方法，给出整体测评的具体结果。	符合	部分符合	不符合	不适用
3850	多项选择题	根据GM/T 0116《信息系统密码应用测评过程指南》，整体测评过程中，针对测评对象“部分符合”及“不符合”要求的单个测评项，分析与该测评项相关的（　）的测评对象能否和它发生关联关系，发生何种关联关系，这些关联关系产生的作用是否可以“弥补”该测评项的不足，以及该测评项的不足是否会影响与其有关联关系的其他测评项的测评结果。	其他测评对象	其他测评项	其他单元	其他层面
3851	多项选择题	根据GM/T 0116《信息系统密码应用测评过程指南》，以下关于量化评估工作的说明，正确的是（　）。	各测评单元得分需要根据各个测评对象的符合程度得分进行计算	各安全层面的得分需要根据各测评单元的得分进行计算	根据单元测评结果直接计算整体得分	根据各测评单元、各层面和整体得分，总体评价被测信息系统已采取的有效保护措施和存在的密码应用安全问题情况。
3852	多项选择题	根据GM/T 0116《信息系统密码应用测评过程指南》，根据（　），判断测评结果汇总中部分符合项或不符合项所产生的安全问题被威胁利用的可能性，可能性的取值范围为高、中和低。	威胁发生频率	威胁类型	自身水平	量化评估结果
3853	多项选择题	根据GM/T 0116《信息系统密码应用测评过程指南》，风险分析在（　）信息的基础上进行。	被测系统威胁分析结果	被测系统资产分析结果	被测系统存在的安全问题	已有安全措施情况

3854	多项选择题	根据GM/T 0116《信息系统密码应用测评过程指南》，测评方根据（ ）等相关标准要求，对被测信息系统面临的密码应用安全风险进行赋值，风险值的取值范围为高、中和低。	单元测评结果	自身经验	《信息系统密码应用高风险判定指引》	整体测评结果
3855	多项选择题	根据GM/T 0116《信息系统密码应用测评过程指南》，关于资产和威胁评估，说法正确的是（ ）。	资产价值的认定，是依据资产价格来决定	资产价值越高表明资产遭到威胁时将导致越高的风险	威胁发生频率越高表明资产的安全越有可能受到威胁	资产价值高低的界定可由测评委托单位根据密码应用方案、等级保护定级报告等继承和确定，并由测评结构进行审查和确认
3856	多项选择题	根据GM/T 0116《信息系统密码应用测评过程指南》，密码应用安全性评估过程中在分析与报告编制阶段，通过（ ）环节，找出整个系统密码安全保护现状和相应等级保护要求之间的差距。	单项测评结果判定	单元测评结果判定	整体测评	风险分析
3857	多项选择题	根据GM/T 0116《信息系统密码应用测评过程指南》，评估结论需要在（ ）的基础上形成。	整体测评	测评结果汇总	量化评估	风险分析
3858	多项选择题	以下关于评估结论的描述正确的是（ ）。	符合：被测信息系统中未发现安全问题，测评结果中所有单元测评结果中部分符合和不符合项的统计结果全为0，综合得分为100分。	基本符合：被测信息系统中存在安全问题，部分符合和不符合项的统计结果不全为 0，且综合得分不低于阈值。	不符合：被测信息系统中存在安全问题，部分符合和不符合项的统计结果不全为0，综合得分低于阈值。	不符合：被测信息系统存在的安全问题会导致 被测信息系统面临高等级安全风险。
3859	多项选择题	根据GM/T 0116《信息系统密码应用测评过程指南》，被测信息系统的密评结论可能是（ ）。	符合	部分符合	不符合	基本符合

3860	多项选择题	根据GM/T 0116《信息系统密码应用测评过程指南》，密评报告应符合信息系统密码应用安全性评估报告模板要求，包括但不限于以下内容（）。	测评项目概述、被测系统情况	测评范围与方法	整体测评、量化评估	评估结论、安全问题及改进建议
3861	多项选择题	根据GM/T 0116《信息系统密码应用测评过程指南》，密评报告编制完成后，测评方应根据（）对密评报告进行内部评审。	测评原始记录	被测单位提交的相关文档	其他辅助信息	委托测评协议书
3862	多项选择题	根据GM/T 0116《信息系统密码应用测评过程指南》，以下哪些属于密评报告的内容（ ）。	整体测评	量化评估	评估结论	总体评价
3863	判断题	根据GM/T 0116《信息系统密码应用测评过程指南》，测评方对信息系统开展密码应用安全性评估时，应遵循不可重复性原则。	正确	错误		
3864	判断题	根据GM/T 0116《信息系统密码应用测评过程指南》，开展密码应用安全性评估时，可重用性原则要求所有重用结果都应以已有测评结果仍适用于当前被测信息系统为前提，并能够客观反映系统当前的安全状态。	正确	错误		
3865	判断题	根据GM/T 0116《信息系统密码应用测评过程指南》，密码应用安全性评估遵循的基本原则有客观公正原则、经济性原则、可重复性和可再现性原则、结果完善性原则。	正确	错误		
3866	判断题	根据GM/T 0116《信息系统密码应用测评过程指南》，密评的可重复性原则是：按照同样的要求、使用同样的测评方法、在同样的环境下，不同测评人员对同一个测评实施过程的重复执行应得到同样的结果。	正确	错误		

3867	判断题	根据GM/T 0116《信息系统密码应用测评过程指南》，密评的可再现性原则是：按照同样的要求、使用同样的测评方法、在同样的环境下，同一测评人员对每个测评实施过程的重复执行应得到同样的结果。	正确	错误		
3868	判断题	根据GM/T 0116《信息系统密码应用测评过程指南》，A系统部署的物理环境现状的密评结果已包含在B系统的密评报告中，则A系统密评时可复用B系统密评报告中的相应评估结果。	正确	错误		
3869	判断题	根据GM/T 0116《信息系统密码应用测评过程指南》，测评工作的开展可能会给被测信息系统带来一定风险，测评方应在测评开始前完成全部风险识别工作。	正确	错误		
3870	判断题	根据GM/T 0116《信息系统密码应用测评过程指南》，现场测评之前，测评方应与被测单位签署现场测评授权书，要求测评相关方对系统及数据进行备份，并针对可能出现的事件制定应急处理方案。	正确	错误		
3871	判断题	根据GM/T 0116《信息系统密码应用测评过程指南》，现场测评过程中，如果被测系统配置了与被测信息系统一致的模拟/仿真环境，可以在模拟/仿真环境下开展验证测试和工具测试工作。	正确	错误		
3872	判断题	根据GM/T 0116《信息系统密码应用测评过程指南》，在测评活动开展前，需要对被测信息系统的密码应用方案进行评估，密码应用方案可以作为测评实施的依据。	正确	错误		

3873	判断题	根据GM/T 0116《信息系统密码应用测评过程指南》，测评过程中的分析与报告编制活动的实施顺序是：单元测评、整体测评、量化评估、风险分析、密评报告编制、评估结论形成。	正确	错误		
3874	判断题	根据GM/T 0116《信息系统密码应用测评过程指南》，方案编制活动是开展测评工作的关键活动，主要任务是编写收集确认信息系统的资产信息，并确定与被测信息系统相适应的测评对象、测评指标、测评检查点及测评内容，形成密评方案，为实施现场测评提供依据。	正确	错误		
3875	判断题	根据GM/T 0116《信息系统密码应用测评过程指南》，密码应用安全性评估基本测评活动包括测评准备活动、方案编制活动、现场测评活动、分析与报告编制活动。	正确	错误		
3876	判断题	根据GM/T 0116《信息系统密码应用测评过程指南》，测评准备活动由信息收集和分析、工具和表单准备两项主要任务组成。	正确	错误		
3877	判断题	根据GM/T 0116《信息系统密码应用测评过程指南》，在测评准备阶段进行是信息收集和分析的过程中，测评方分析调查结果，可以采信自查结果、上次网络安全保护等级测评报告或商用密码应用安全性评估报告中的可信结果。	正确	错误		
3878	判断题	根据GM/T 0116《信息系统密码应用测评过程指南》，校准本次测评过程中可能用到的测评工具，发生在现场测评活动中。	正确	错误		

3879	判断题	根据GM/T 0116《信息系统密码应用测评过程指南》，如果具备条件，建议密评人员模拟被测信息系统搭建测评环境，进行前期准备和验证。	正确	错误		
3880	判断题	根据GM/T 0116《信息系统密码应用测评过程指南》，为确保密评结果的准确性，应针对生产系统进行密评，避免使用搭建的测试环境。	正确	错误		
3881	判断题	根据GM/T 0116《信息系统密码应用测评过程指南》，密评工作中，如果测评准备阶段调查表格中存在相互矛盾的情况，密评人员应与填表人进行沟通和确认，但测评方应尽量避免现场调查，影响系统运行。	正确	错误		
3882	判断题	根据GM/T 0116《信息系统密码应用测评过程指南》，密评工作的测评准备活动中，到被测信息系统现场进行信息收集的过程是必须的。	正确	错误		
3883	判断题	根据GM/T 0116《信息系统密码应用测评过程指南》，密评工作中，工具和表单准备阶段输出物的内容应涵盖测评工具、现场测评授权、测评可能带来的风险、交接的文档名称、会议记录表单、会议签到表单等。	正确	错误		
3884	判断题	根据GM/T 0116《信息系统密码应用测评过程指南》，在密码应用安全性评估活动中，确定测评对象和测评指标是测评准备活动的内容。	正确	错误		
3885	判断题	根据GM/T 0116《信息系统密码应用测评过程指南》，测评方案编制活动中，测评对象确定需要基于完成的调查表格、以及各种与被测信息系统相关的技术资料，并最终确认密评方案中的测评对象。	正确	错误		

3886	判断题	根据GM/T 0116《信息系统密码应用测评过程指南》，无论信息系统密码应用方案是否通过评估，测评方均需要对所有不适用项进行逐条核查、评估，论证其安全需求、不适用的具体原因，以及是否采用了可满足安全要求的其他替代性风险控制措施来达到等效控制。	正确	错误		
3887	判断题	根据GM/T 0116《信息系统密码应用测评过程指南》，对于“宜”的指标，若信息系统的密码应用方案通过评估且方案中做了明确的不适用说明，可不纳入测评范围。	正确	错误		
3888	判断题	根据GM/T 0116《信息系统密码应用测评过程指南》，确定测评检查点需充分考虑检查的可行性和风险，最大限度的避免对被测信息系统的影响。	正确	错误		
3889	判断题	根据GM/T 0116《信息系统密码应用测评过程指南》，在使用工具进行测评时应在保证被测信息系统正常、安全运行的情况下，确定测试路径和工具接入点，并结合网络拓扑图，采用图示的方式描述测评工具的接入点、测试目的、测试途径和测试对象等相关内容。	正确	错误		
3890	判断题	根据GM/T 0116《信息系统密码应用测评过程指南》，在使用工具进行测评时应在保证被测信息系统正常、安全运行的情况下，确定测试路径和工具接入点，当测评工具接入被测信息系统条件不成熟时，测评方应搭建测试模拟环境进行接入测试。	正确	错误		
3891	判断题	根据GM/T 0116《信息系统密码应用测评过程指南》，测评检查点确定主要任务为确定工具测试的接入点、测试途径、测试目的。	正确	错误		

3892	判断题	根据GM/T 0116《信息系统密码应用测评过程指南》，在密评工作中，测评内容的确定是将测评对象与测评指标，测评对象与测评方法联系起来的过程。	正确	错误		
3893	判断题	根据GM/T 0116《信息系统密码应用测评过程指南》，编写完成的信息系统密评方案应该在提交被测单位并进行签字确认后，进行测评方内部评审。	正确	错误		
3894	判断题	根据GM/T 0116《信息系统密码应用测评过程指南》，密评人员在现场测试结束后，应保持现场环境的测评状态，以便核对测评结果。	正确	错误		
3895	判断题	根据GM/T 0116《信息系统密码应用测评过程指南》，某密评人员在现场测试过程中生成了测试账号，现场测试结束后在委托方配合下清除了测试账号及关联数据，以上做法是正确的。	正确	错误		
3896	判断题	根据GM/T 0116《信息系统密码应用测评过程指南》，现场测评活动的目标是通过与被测单位进行沟通和协调，依据密评方案实施现场测评工作，获取分析与报告编制活动所需且足够的证据和资料。	正确	错误		
3897	判断题	密评实施过程中，需要深入验证密码产品的功能实现，并核查密码产品是否在信息系统中正确、有效地发挥作用。	正确	错误		
3898	判断题	根据GM/T 0116《信息系统密码应用测评过程指南》，进行配置检查时，根据被测单位出具的商用密码产品认证证书（复印件）、安全策略文档或用户手册等，先确认实际部署的密码产品与声称情况的一致性，再查看配置的正确性，并记录相关证据。	正确	错误		

3899	判断题	根据GM/T 0116《信息系统密码应用测评过程指南》，对于已经取得商用密码产品认证证书的密码产品，测评时不对其本身进行重复检测，主要进行符合性核验和配置检查。	正确	错误		
3900	判断题	根据GM/T 0116《信息系统密码应用测评过程指南》，进行工具测试时，需根据测评机构的实际情况选择测试工具，在配置检查无法提供有力证据的情况下，应通过工具测试的方法抓取并分析被测信息系统相关数据。	正确	错误		
3901	判断题	根据GM/T 0116《信息系统密码应用测评过程指南》，现场测评过程中，若无法在密码产品和调用者之间接入测试工具、且被测信息系统无法提供源代码等有关证据的情况下，可通过逆向分析等方法对被测信息系统应用程序进行逆向分析，探究应用程序内部组成结构及工作原理，核查应用程序调用密码功能的合理性。	正确	错误		
3902	判断题	根据GM/T 0116《信息系统密码应用测评过程指南》，现场测评时，对于已经取得相应证书的密码产品，确认实际部署的密码产品与声称产品的一致性后，可不进行其他测评。	正确	错误		
3903	判断题	根据GM/T 0116《信息系统密码应用测评过程指南》，测评结果确认和资料归还部分输出文档的内容为测评活动中发现的问题、问题的证据和证据源、每项测评活动中被测单位配合人员的书面认可文件。	正确	错误		

3904	判断题	根据GM/T 0116《信息系统密码应用测评过程指南》，密评人员在初步判定各测评单元涉及的各个测评对象的测评结果后，还需进行单元测评、整体测评、量化评估和风险分析。经过整体测评后，如果发现测评对象的测评结果有所变化，需进一步修订测评结果，而后进行量化评估和风险分析，最后形成评估结论。	正确	错误		
3905	判断题	根据GM/T 0116《信息系统密码应用测评过程指南》，由于信息系统测评对象较多，可能导致不同测试人员针对同一测评单元得出的测评结果存在差异。	正确	错误		
3906	判断题	根据GM/T 0116《信息系统密码应用测评过程指南》，测评单元包含的所有测评对象的测评结果均为符合或部分符合，则对应测评单元结果判定为符合。	正确	错误		
3907	判断题	根据GM/T 0116《信息系统密码应用测评过程指南》，测评单元包含的所有测评对象的测评结果不全为符合，则对应测评单元结果判定为不符合。	正确	错误		
3908	判断题	根据GM/T 0116《信息系统密码应用测评过程指南》，测评单元包含的所有测评对象的测评结果均为不适用，则对应测评单元结果判定为不适用。	正确	错误		
3909	判断题	根据GM/T 0116《信息系统密码应用测评过程指南》，整体测评是对各个单元测评结果进行汇总分析，统计符合情况。	正确	错误		

3910	判断题	根据GM/T 0116《信息系统密码应用测评过程指南》，层面间测评是指对同一技术层面或管理方面内的两个或者两个以上不同测评单元间的关联进行测评分析。	正确	错误		
3911	判断题	根据GM/T 0116《信息系统密码应用测评过程指南》，整体测评任务针对测评结果为符合、部分符合和不符合的测评对象，采取逐条判定的方法，给出整体测评的具体结果。	正确	错误		
3912	判断题	根据GM/T 0116《信息系统密码应用测评过程指南》，整体测评过程中，针对测评对象“部分符合”及“不符合”要求的单个测评项，分析与该测评项相关的其他测评项、其他单元、其他层面的测评对象能否和它发生关联关系，发生何种关联关系，这些关联关系产生的作用是否可以“弥补”该测评项的不足，以及该测评项的不足是否会影响与其有关联关系的其他测评项的测评结果。	正确	错误		
3913	判断题	根据GM/T 0116《信息系统密码应用测评过程指南》，层面间测评是指对不同层面内的两个或者两个以上测评单元间的关联关系进行测评分析。	正确	错误		
3914	判断题	根据GM/T 0116《信息系统密码应用测评过程指南》，根据单元测评结果，计算各测评指标的各个测评对象的测评结果符合程度得分，之后再进行整体测评。	正确	错误		

3915	判断题	根据GM/T 0116《信息系统密码应用测评过程指南》，在量化评估任务中，针对测评对象“部分符合”及“不符合”要求的单个测评项，可以通过不同单元的测评对象直接的关联关系，分析这些关联关系产生的作用是否可以“弥补”某一测评项的不足。	正确	错误		
3916	判断题	根据GM/T 0116《信息系统密码应用测评过程指南》，量化评估任务的定义是：综合单元测评结果和整体测评结果，计算修正后的各测评指标的各个测评对象的测评结果得分、各测评单元得分、各安全层面得分和整体得分，并对被测信息系统的密码应用情况安全性进行总体评价。	正确	错误		
3917	判断题	根据GM/T 0116《信息系统密码应用测评过程指南》，测评方根据自身经验、相关标准或文件，对被测信息系统面临的密码应用安全风险进行赋值，风险值的取值范围为高、中和低。	正确	错误		
3918	判断题	根据GM/T 0116《信息系统密码应用测评过程指南》，测评方应根据自身经验对被测信息系统面临的密码应用安全风险进行赋值。	正确	错误		
3919	判断题	被测信息系统中存在安全问题，部分符合项和不符合项的统计结果不全为0，且综合得分不低于阈值，被测系统的密评结论可判定为基本符合。	正确	错误		
3920	判断题	被测信息系统中存在安全问题，部分符合和不符合项的统计结果不全为0，而且存在的安全问题会导致被测信息系统面临高等级安全风险，且综合得分低于阈值，被测系统的密评结论可判定为基本符合。	正确	错误		

3921	判断题	某信息系统整体量化评估结果为70分，且风险评估未发现高风险，因此该系统的密评结论应为部分符合。	正确	错误		
3922	判断题	某信息系统整体量化评估结果为70分，且漏洞扫描未发现高危漏洞，因此该系统的密评结论应为部分符合。	正确	错误		
3923	单项选择题	针对管理制度层面的“定期修订安全管理制度”指标要求，密评时主要是通过访谈安全主管，确定是否定期对密码安全管理制度体系的（ ）进行审定。	合理性和适用性	合理性和完备性	合理性和灵活性	合理性和通用性
3924	单项选择题	某信息系统通过堡垒机对设备进行集中运维管理，堡垒机采用动态令牌进行身份鉴别。则对该设备的身份鉴别主要测评的内容包括（ ）。	无需测评动态令牌系统产品的合规性	如果设备是合规的密码产品，则无需测评，直接判为符合	如果设备不是合规的密码产品，则无需测评，直接判为不符合	根据实际情况核验该设备的身份鉴别实现机制
3925	单项选择题	某信息系统在互联网边界部署安全认证网关，为用户访问应用建立起安全的通信信道。互联网用户客户端并未部署数字证书，则在网络和通信安全层面，对互联网用户访问应用的网络通信信道的测评的内容是（ ）。	互联网客户端和安全认证网关之间的身份鉴别、通信数据机密性和完整性	互联网客户端和应用服务器之间的身份鉴别、通信机密性和完整性	安全认证网关和应用服务器之间的身份鉴别、通信数据机密性和完整性	应用服务器和第三方电子认证服务机构之间的身份鉴别、通信数据机密性和完整性
3926	单项选择题	某信息系统设备管理员在互联网通过SSL VPN访问内网后，再登录堡垒机对设备进行运维管理，运维人员在互联网通过智能密码钥匙登录SSL VPN；则在网络和通信安全层面，对该远程管理通道的主要测评的内容包括（ ）。	运维客户端和SSL VPN之间的身份鉴别、通信机密性和完整性	运维客户端和堡垒机之间的身份鉴别、通信机密性和完整性	SSL VPN和堡垒机之间的身份鉴别、通信机密性和完整性	堡垒机和服务器之间的身份鉴别、通信机密性和完整性

3927	单项选择题	某信息系统设备管理员在互联网通过SSL VPN接入内网后，再登录堡垒机对设备进行运维管理，同时在SSL VPN后部署了防火墙进行网络访问控制；则在网络和通信安全层面，针对“网络边界访问控制信息的完整性”测评要求的测评对象为（ ）。	防火墙上的网络边界访问控制信息	SSL VPN上的网络边界访问控制信息	堡垒机上的网络边界访问控制信息	服务器上的网络边界访问控制信息
3928	单项选择题	以下属于应用和数据安全层面，业务应用访问控制信息完整性指标测评内容的是（ ）。	SSL VPN中的访问控制列表	应用系统的权限	服务器的系统权限访问控制信息	防火墙的访问控制列表
3929	单项选择题	在对应用和数据安全中的“重要数据存储完整性”测评时，以下哪个密码技术量化评估得分无法达到1分（ ）。	使用SM3算法计算杂凑值	使用SM3、SM2算法计算签名值	使用HMAC-SM3算法计算消息鉴别码	使用SM4- CBC模式生成消息鉴别码，其中初始向量为全0，消息长度为约定好的固定长度
3930	单项选择题	密评人员在对关键设备进行现场检查时，测评工具接入被测信息系统条件不成熟，测评方应（ ）。	模拟被测信息系统搭建测评环境获取测评数据	与被测单位协商、配合，生成必要的离线数据	告知被测单位风险后，接入被测系统获取真实数据	将该测评项做不适用处理
3931	多项选择题	对于未标注密码模块安全等级的商用密码产品在现场测评时应考虑以下哪些因素（ ）。	分析其是否为换证密码产品，对于换证的密码产品，需要密码厂商进一步提供换证前的商用密码产品型号证书，如果商用密码产品型号证书中标注了其符合的密码模块等级，则按此等级进行判定	对于换证的密码产品，需要密码厂商进一步提供换证前的商用密码产品型号证书，如果商用密码产品型号证书中未标注其符合的密码模块等级，按“密码产品符合一级密码模块”进行判定	分析其是否为新认证密码产品，对于新发认证证书的密码产品，需核实其是否为适用于密码模块标准的密码产品	若为密码系统类产品（如电子签章系统等），则其不适用于密码模块标准，但作为系统组件的密码产品则适用于密码模块标准，在密评时依据这些密码产品的密码模块安全等级进行判定

3932	多项选择题	对运行在云平台上的云上应用进行密评时，特别是云平台和云上应用的运营者不同的情况下，关于两者的责任和范围界定，以下表述合理的是（）。	针对云平台自身密评，该部分测评的责任主体为云平台的运营者	针对云上应用系统的密评，该部分测评的责任主体为云上应用的运营者	云上应用系统所处的云平台通过密评（即获得“符合”或“基本符合”的结论）后，云上应用系统才能通过密评	云上应用系统所处的云平台的安全级别应不低于云上应用系统
3933	多项选择题	GB/T 39786《信息安全技术 信息系统密码应用基本要求》中，信息系统安全管理方面的要求都包括（）。	管理制度要求	人员管理要求	建设运行要求	应急处置要求
3934	多项选择题	设备和计算安全层面，关于密码设备的“身份鉴别”测评指标要求，需核验、测试以下哪些内容（）。	判断该密码产品是否为经检测认证合格的商用密码产品	确认实际部署的密码产品与获证产品是否一致	核查密码产品是否采用了智能IC卡、智能密码钥匙、动态口令等技术对登录设备的管理员进行身份鉴别	验证是否按照密码产品使用要求对登录设备的用户使用密码技术进行身份鉴别
3935	多项选择题	下列内容属于设备和计算安全层面系统资源访问控制信息的是（）。	SSL VPN设备的系统权限访问控制信息	运维堡垒机的系统访问控制信息	数据库中的数据访问控制信息	应用系统的权限
3936	多项选择题	在网络和通信安全层面，访问控制信息主要包括哪些（）。	部署在网络边界的VPN中的访问控制列表	部署在网络边界的防火墙的访问控制列表	部署在网络边界的边界路由的访问控制列表	部署在应用域的安全网关的访问控制信息
3937	多项选择题	双活机房之间通信的通信链路，在测评时是否作为网络和通信安全层面的一条通信信道，以下表述正确的是（）。	因重要业务数据、重要个人信息等数据会在双活机房之间进行传输，应将该通信信道作为测评对象	双活机房之间的通信链路采用运营商专线时应将该通信信道作为测评对象	双活机房之间的通信链路采用物理裸光纤时原则上应将该通信信道作为测评对象	如果双活机房之间通信的通信链路是纯物理传输的裸光纤，若不将该通信信道作为网络和通信安全层面的测评对象，应通过专家评审。

3938	多项选择题	某三级信息系统运维人员从互联网，通过SSL VPN接入内网后，再登录堡垒机对系统中的服务器进行远程运维管理，运维人员均配置了智能密码钥匙，则在网络和通信安全层面的“身份鉴别”的主要测评内容包括（ ）。	客户端对SSL VPN服务端的身份鉴别	SSL VPN服务端对客户端使用智能密码钥匙的身份鉴别	第三方电子认证服务	身份鉴别过程是否采用了挑战响应机制
3939	多项选择题	网络和通信安全、应用和数据安全都有传输安全性（机密性、完整性）的要求，以下说法正确的是（ ）。	如果网络和通信安全层面合规，应用和数据安全层面的传输机密性和完整性未采用密码技术，则网络层可以缓解应用层传输安全的风险	如果应用和数据安全层面的某关键数据传输机密性和完整性符合要求，网络和通信安全层面未采用密码技术，则应用层可以弥补网络层的传输安全	两个安全层面的数据保护对象不一样	两个安全层面可以相互弥补，降低风险
3940	多项选择题	信息系统已确认采用经检测认证合格的商用密码产品实现密钥管理安全，对密钥管理的安全性判定还需现场核查以下哪些内容（ ）。	根据信息系统的安全级别，该密码产品的密码模块安全级别是否满足GB/T 39786《信息安全技术 信息系统密码应用基本要求》相应安全等级的要求	如果被测系统有密码应用方案，应核查系统密钥管理机制是否与方案一致	由密码产品产生的密钥在该密码产品外部进行管理时，是否进行了机密性和完整性保护	该密码产品是否按照产品配套的安全策略文档进行部署和使用

3941	多项选择题	面向公众，信息可公开的信息系统，测评时需要重点关注以下哪些内容（ ）。	首先需要确定哪些人员可以访问该信息系统	管理员的身份鉴别、传输通道安全及其遵循的测评指标	对于公众用户而言，仍需要对网站进行身份鉴别（比如防止钓鱼网站），并对其内容的完整性进行保护	需要测评与公众用户相关的“网络和通信安全”层面的“身份鉴别”、“通信过程中数据的完整性”、“通信过程中重要数据的机密性”等指标
3942	多项选择题	某办公系统部署了SSL VPN安全网关，并向相关用户配发USBKey，通过非国密浏览器实现对PC端登录系统用户的身份鉴别，在密码应用安全性评估时应重点测评内容包括（ ）。	核查SSL VPN安全网关合规性	核查USBKey合规性	核查PC端浏览器合规性	验证身份鉴别机制是否正确和有效
3943	判断题	在设备和计算安全层面，“采用密码技术保证系统资源访问控制信息的完整性”的指标要求，强调的是被测设备的系统资源。	正确	错误		
3944	判断题	某三级信息系统通过堡垒机对系统中的服务器进行集中运维管理，堡垒机采用动态令牌进行身份鉴别，则对服务器的身份鉴别为主要测评动态令牌的合规性。	正确	错误		
3945	判断题	某信息系统所在机房部署使用的电子门禁系统为经检测认证合格的密码产品，则可判定该电子门禁系统的电子门禁记录数据存储完整性指标为符合。	正确	错误		
3946	判断题	某信息系统所在机房的视频监控系统是一个密码产品，采集端到服务端采用了密码技术实现了通信数据的机密性和完整性保护，则可判定该机房的视频监控记录数据存储完整性指标为符合或部分符合。	正确	错误		

3947	判断题	在应用和数据安全中，“采用密码技术保证信息系统应用的访问控制信息的完整性”指标要求，强调的是系统应用。	正确	错误		
3948	判断题	在应用和数据安全层面，访问控制信息主要包括应用系统的权限、标签等能够决定系统应用访问控制的措施等信息。	正确	错误		
3949	判断题	根据《商用密码应用安全性评估FAQ（第二版）》，信息系统采用经认证合格的密码产品是密钥管理安全性（D）判定为“符合”的必要条件。	正确	错误		
3950	单项选择题	针对已上线运行信息系统，在对其进行安全管理层面测评时，其测评对象包括系统相关人员、安全管理制度文档、记录表单和（ ）。	密码应用安全性评估文档	立项规划文档	技术标准	建设实施方案文档
3951	单项选择题	针对整机类密码产品（如IPSec VPN网关、SSL VPN网关、安全认证网关、金融数据密码机、服务器密码机、签名验签服务器、时间戳服务器、云服务器密码机等），以( )为粒度确定设备和计算安全层面的测评对象。	具有相同硬件、软件配置的设备	具有相同商用密码产品认证证书编号的密码产品	具有相同功能的密码产品	相同类型的密码产品
3952	单项选择题	某信息系统部署了服务器C三台服务器，三台服务器为同一批次购买，生产厂商、型号和操作系统版本等都相同，购买后，A和B的操作系统升级为了相同的版本，则（ ）。	C作为3个不同的测评对象	A和B作为一个测评对象，C为另一个测评对象	ABC作为一个测评对象	A和C作为一个测评对象，B为另一个测评对象
3953	单项选择题	某信息系统部署了B两台服务器，其生产厂商、型号和操作系统版本等都相同，购买后对服务器A的身份鉴别进行了改造，测评时对服务器的身份鉴别量化评估方法为（ ）。	D/A/K均以两个服务器的实际应用情况各自赋分	D/A/K均以未改造服务器B的实际应用情况赋分	D/A/K均以未改造服务器A的实际应用情况赋分	依据被测单位要求对服务器赋分

3954	单项选择题	某三级信息系统运维管理员通过互联网直接访问堡垒机，对设备进行运维管理，则管理员通过互联网访问堡垒机的通信信道（ ）。	仅作为网络和通信安全层面的测评对象	仅作为设备和计算安全层面“远程管理通道安全”的测评对象	可作为网络和通信安全层面、设备和计算安全层面“远程管理通道安全”的测评对象	不可作为网络和通信安全层面、设备和计算安全层面“远程管理通道安全”的测评对象
3955	单项选择题	某三级信息系统运维管理员客户端通过互联网访问VPN接入内网后，再登录堡垒机对通用服务器进行运维管理，则在设备和计算安全层面，通用服务器的“远程管理通道安全”测评指标的测评对象是（ ）。	客户端至VPN间的信道	VPN至堡垒机间的信道	堡垒机至通用服务器间的信道	以上都是
3956	单项选择题	某三级信息系统中，应用包括前台应用系统和后台管理系统；系统运行的网络环境通常包括互联网、政务外网和办公内网，其中，办公内网也属于政务外网。该信息系统网络通信情况描述如下： (1) 用户可以从互联网、政务外网、办公内网，使用非国密浏览器或国密浏览器通过HTTPS协议访问前台应用系统；(2) 管理员可以从办公内网或使用VPN客户端通过内网SSLVPN接入办公内网后，再使用国密浏览器通过HTTPS协议访问后台管理系统；(3) 系统管理员可以从互联网先登录运维专用的SSLVPN后，再通过堡垒机对服务器、密码产品等设备进行运维；(4) 信息系统可以通过IPSec VPN调用外部的密码资源（例如政务外网的数据加密服务）。根据以上描述，此信息系统网络和通信安全层面的测评对象包括多少个通信信道（ ）。	5	6	7	8

3957	单项选择题	政务信息系统中，已经确定的测评对象是政务外网SSL VPN客户端与内网SSL VPN之间的通信信道，则其密码应用场景是（ ）。	管理员用户从政务外网通过内网SSL VPN接入办公内网	管理员从办公内网使用国密浏览器通过HTTPS协议访问内网应用	用户从政务外网使用非国密浏览器通过HTTPS协议访问内网应用	用户从互联网使用非国密浏览器通过HTTPS协议访问内网应用
3958	单项选择题	政务信息系统中，已经确定的测评对象是互联网国密浏览器与前台应用系统之间的通信信道，则其密码应用场景是（ ）。	用户从互联网使用国密浏览器通过HTTPS协议访问前台应用系统	用户从政务外网使用国密浏览器通过HTTPS协议访问前台应用系统	用户从互联网使用非国密浏览器通过HTTPS协议访问前台应用系统	用户从政务外网使用非国密浏览器通过HTTPS协议访问前台应用系统
3959	单项选择题	应用和数据安全要求中“采用密码技术对登录用户进行身份鉴别，保证应用系统用户身份的真实性”的用户指的是（ ）。	所有登录设备的实体	所有登录应用进行操作的实体	设备管理员	应用管理员
3960	单项选择题	某第三级信息系统包括两个重要应用，其中A应用中包括两类不同角色的用户，B应用包括三类不同角色管理员用户，且这些用户之间的的身份鉴别方式均不相同，那么“应用和数据安全”的“身份鉴别”测评时，分为几个测评对象最为合理（ ）。	2	3	4	5
3961	单项选择题	使用IPSec协议分析工具抓包，主要抓取并分析的是哪个阶段的数据包（ ）。	握手阶段数据包	密钥交换协议第一阶段的数据包	密钥交换协议第二阶段的数据包	安全报文协议
3962	单项选择题	政务信息系统中，已经确定的测评对象是办公内网国密浏览器与后台管理系统之间的通信信道，则其场景是（ ）。	用户从政务外网使用国密浏览器通过HTTPS协议访问前台应用系统	系统管理员从互联网访问SSL VPN运维设备	用户从政务外网使用非国密浏览器通过HTTPS协议访问前台应用系统	管理员从办公内网使用国密浏览器通过HTTPS协议访问后台管理系统
3963	单项选择题	关于云平台“被部分评估的支撑能力”描述错误的是（　）。	“被部分评估的支撑能力表”只在云平台测评时填写	“被部分评估的支撑能力表”包含有适用条件的量化评估和风险分析	被部分评估的支撑能力只需在云平台测评	被部分评估的支撑能力主要指的是对云上应用提供的密码支撑服务

3964	单项选择题	政务信息系统中，已经确定的测评对象是政务外网IPSec VPN与IPSec VPN之间的通信信道，则其场景是（ ）。	用户从政务外网使用非国密浏览器通过HTTPS协议访问前台应用系统	系统管理员从互联网访问SSL VPN运维设备	管理员从办公内网使用国密浏览器通过HTTPS协议访问后台管理系统	信息系统从政务外网通过IPSec VPN调用外部密码资源
3965	单项选择题	如果服务器只能进行本地运维，采用用户名/口令方式进行身份鉴别，则可降低风险的缓解手段不包括（ ）。	基于特定设备识别技术保证用户身份的真实性	机房测评合规且有严格的机房管理制度	基于生物指纹技术保证用户身份的真实性	服务器单独安装在具有良好安防措施的密闭区域且只有运维人员才有权限访问
3966	单项选择题	某一信息系统部署了5台IPSec VPN，均具有商用密码产品认证证书，其中3台编号均为GM001110620202027，2台编号为GM001110620202036，设备和计算安全层面有（ ）个IPSEC VPN测评对象。	2	3	5	8
3967	单项选择题	某机关办公OA信息系统面向机关内所有办公人员提供服务，信息系统系统通过管理员进行运行维护。经测评，如果办公人员身份鉴别判定为不符合，管理员身份鉴别判定为符合，针对应用和数据层面的“身份鉴别”测评单元，最终判定结果为（ ）。	部分符合	符合	不符合	不适用
3968	单项选择题	对于已更换商用密码产品认证证书的密码产品如果未标注密码模块安全等级，以下描述错误的是（ ）。	需要进一步提供换证前的商用密码产品型号证书	需要确认换证前的商用密码产品型号证书的安全等级是否符合要求	未提供安全等级证明的按照“密码产品等级不符合”进行判定	提供密码产品的密钥管理安全措施方案，证明其符合安全要求，并按“密码产品等级符合”判定

3969	单项选择题	具有商用密码产品认证证书的密码产品，且实际部署与认证通过时的状态一致的情况下，对密码产品可以直接判定为符合的指标是（　）。	身份鉴别	系统资源访问控制信息完整性	日志记录完整性	重要可执行程序完整性、重要可执行程序来源真实性
3970	单项选择题	管理员在互联网通过SSL VPN接入系信息统内网，再登录堡垒机后采用SSH协议对设备进行远程管理，则在网络和通信安全层面的测评对象为（）。	浏览器与SSL VPN之间的通信信道	堡垒机与设备之间的通信信道	浏览器与堡垒机之间的通信信道	浏览器与设备之间的通信信道
3971	单项选择题	某信息系统部署在公有云平台的独立VPC内，管理员在互联网通过浏览器访问云平台的堡垒机对设备进行远程管理，则在网络和通信安全层面的测评对象为（）。	堡垒机与设备之间的通信信道	浏览器与堡垒机之间的通信信道	浏览器与设备之间的通信信道	设备与设备之间的通信信道
3972	单项选择题	某信息系统的安全等级为第三级，被测单位认为网络与通信安全层面的安全接入认证不适用，则应在设计密码应用方案时（）。	不需要明确说明安全接入认证指标的不适用性	需要明确说明安全接入认证指标的不适用性，并且需要采取风险控制措施	需要明确说明安全接入认证指标的不适用性，但不需要采取风险控制措施	无法作为不适用项
3973	单项选择题	如果被测信息系统所在的物理机房采用多区域部署或被测信息系统重要资产分布在不同的物理机房中，物理和环境测评对象包括（）。	仅密码设备所在机房	所有该信息系统涉及的机房	主机房	具有门禁和视频监控系统的机房
3974	单项选择题	对信息系统应用和数据安全层面测评时，针对日志记录完整性的测评对象包括应用系统、密码产品、技术文档和（）。	安全审计员	系统管理员	系统操作员	保密员
3975	单项选择题	对第三级信息系统的密钥管理安全进行测评时，其测评对象主要包括密钥管理制度、应用系统、密码产品和（）。	系统操作员	系统管理员	安全审计员	密钥管理人员
3976	多项选择题	以下属于云平台被完全评估的支撑能力的是（）。	云机房	密码设备	服务器实体机	虚拟密码设备

3977	多项选择题	密评人员在测评中，发现某密码产品有商用密码产品认证证书，但认证证书已经过期，测评人员应该（　）。	核查密码产品的安全等级	核查相关的密钥管理制度	如果该密码产品产生的密钥在密码产品外管理，核查相应的保护措施	核查购买该密码产品的合同
3978	多项选择题	信息系统可采用以下密码产品保护其应用和数据安全层面的安全：（）	利用智能密码钥匙、智能 IC 卡、动态令牌等作为用户登录应用的凭证。	利用服务器密码机等设备对应用系统指定的重要数据进行加密和计算消息杂凑后传输，实现对重要数据（在应用和数据安全层面）在传输过程中的保密性和完整性保护。	利用服务器密码机等设备对重要数据进行加密、计算 MAC 或签名后存储在数据库中，实现对重要数据在存储过程中的保密性和完整性保护。	利用签名验签服务器、智能密码钥匙、电子签章系统、时间戳服务器等设备实现对可能涉及法律责任认定的数据原发、接收行为的不可否认性
3979	多项选择题	一般情况下，以下不是设备和计算安全层面测评对象的是（）。	交换机	网闸	应用服务器	防火墙（不含密码功能）
3980	多项选择题	某银行金融业务系统重要资产分布在北京主机房、上海业务机房以及苏州灾备机房中，测评时物理和环境测评对象包括（）。	北京主机房	上海业务机房	苏州灾备机房	用户终端所在办公室
3981	多项选择题	设备和计算层面的测评对象主要包括以下哪些（）。	通用服务器（如应用服务器、数据库服务器）	数据库管理系统	整机类和系统类的密码产品	堡垒机（当系统使用堡垒机用于对设备进行集中管理时，不涉及应用和数据安全层面）

3982	多项选择题	对信息系统进行测评时，针对整机类密码产品（如IPSec VPN网关、SSL VPN网关、安全认证网关、金融数据密码机、服务器密码机、签名验签服务器、时间戳服务器、云服务器密码机等）、系统类密码产品（如动态令牌认证系统、证书认证系统、证书认证密钥管理系统等），以下表述正确的是（ ）。	以“具有相同商用密码产品认证证书编号的密码产品”为粒度确定测评对象	具有同一商用密码产品认证证书的密码产品作为一个测评对象	同一厂家密码产品作为一个测评对象	对密码产品类测评对象进行量化评估时，D/A/K均以各测评对象所包含的各个整机类的密码产品或系统类密码产品的实际应用情况的最低分值赋分
3983	多项选择题	对于符合 GM/T 0036-2014《采用非接触卡的门禁系统密码应用技术指南》标准的电子门禁系统，在密评时，以下表述正确的是（ ）。	需要核实是否采用并正确应用了经检测认证合格的电子门禁系统	按照密评相关标准，需要门禁系统厂商进一步提供门禁系统进出记录数据存储完整性保护的相关证据	按照密评相关标准，需要门禁系统厂商进一步提供门禁系统进出记录数据存储机密性保护的相关证据	门禁卡发卡系统可不纳入测试范围
3984	多项选择题	某些信息系统只能在本地进行设备登录运维，但是设备部署在相对安全的机房内部。仅进行本地运维的设备时，针对设备和计算安全层面的“身份鉴别”和“远程管理通道安全”进行测评时，以下表述正确的是（ ）。	测评机构需要首先核实设备确实仅进行本地运行，关闭了对外运维的接口	确保本地端口有效前提下，该测评对象的“远程管理通道安全”测评指标可作为不适用项	“身份鉴别”测评指标为适用项	在对“身份鉴别”测评指标进行测评时，若本地运维均未采用密码技术对登录设备的用户进行身份鉴别，则该测评对象的测评结果为不符合
3985	多项选择题	以下选项中，通常可作为设备和计算安全层面测评对象的是（ ）。	应用服务器	数据库服务器	数据库管理系统	防火墙（不具备密码功能）
3986	多项选择题	管理员在互联网通过SSL VPN接入系统内网，登录堡垒机后采用SSH协议或Telnet协议对设备进行远程管理，则在设备和计算安全层面“远程管理通道安全”分析内容为（ ）。	访问SSL VPN时使用的HTTPS协议	访问堡垒机时使用的HTTPS协议	访问设备时使用的SSH协议	访问设备时使用的Telnet协议

3987	多项选择题	某信息系统部署在公有云平台的独立VPC内，通过云平台的堡垒机对设备进行远程管理，则在设备和计算安全层面“远程管理通道安全”测评单元的测评对象为（ ）。	堡垒机与设备之间的通信信道	浏览器与堡垒机之间的通信信道	浏览器与设备之间的通信信道	设备与设备之间的通信信道
3988	多项选择题	某电商平台包括用户注册业务和商品交易业务两大类，以下选项中属于应用和数据安全层面的测评时关注的内容的是（ ）。	用户注册业务	商品交易业务	交易订单数据	用户浏览记录
3989	多项选择题	以下选项中，属于应用和数据安全层面的重要数据的是（ ）。	鉴别数据	重要业务数据	重要审计数据	个人敏感信息
3990	多项选择题	某电商平台用户需使用合规的智能密码钥匙才能登录，则在应用和数据安全层面“身份鉴别”测评单元的测评对象主要包括（ ）。	电商平台	智能密码钥匙	应用服务器	数据库服务器
3991	多项选择题	某电商平台用户需使用合规的智能密码钥匙才能登录平台，平台采用HTTPS协议进行访问，则在应用和数据安全层面“重要数据传输机密性”测评单元的测评对象主要包括（ ）。	电商平台	智能密码钥匙	提供机密性保护的服务器密码机	数据库服务器
3992	多项选择题	某电商平台用户需使用合规的智能密码钥匙才能登录，平台通过调用服务器密码机对用户注册信息采用SM4算法进行加密存储，则在应用和数据安全层面“重要数据存储机密性”测评单元的测评对象主要包括（ ）。	用户注册信息	智能密码钥匙	服务器密码机	数据库服务器
3993	多项选择题	某信息系统中部署的密码产品包括SSL VPN、服务器密码机等，系统通过堡垒机对服务器进行运维，通过防火墙（不含密码功能）对网络进行访问控制，则设备和计算安全层的测评对象包括（ ）。	SSL VPN	服务器密码机	防火墙（不含密码功能）	堡垒机

3994	多项选择题	某信息系统中部署的密码产品有包括SSL VPN、服务器密码机、智能密码钥匙等，系统通过堡垒机对服务器进行运维，通过防火墙（不含密码功能）对网络进行访问控制，则设备和计算安全层的测评对象包括（ ）。	服务器	服务器密码机	防火墙（不含密码功能）	堡垒机
3995	多项选择题	一般情况下，以下哪些不是设备和计算层面的测评对象（ ）。	防火墙	WAF	网闸	数据库
3996	多项选择题	某整机类密码产品经确认为经检测认证合格的商用密码产品，则在设备和计算安全层面，针对该密码产品的测评，哪些可直接判定为符合（ ）。	身份鉴别	系统资源访问控制信息完整性	重要可执行程序的完整性	日志记录完整性
3997	多项选择题	堡垒机使用合规的智能密码钥匙进行身份鉴别，对通用服务器、数据库进行统一管理，针对通用服务器和数据库采用用户名+口令方式实现身份鉴别的情况，以下关于通用服务器、数据库身份鉴别判定合理的是（ ）。	判定通用服务器和数据库为部分符合	判定通用服务器和数据库为不符合	判定通用服务器和数据库采取了风险缓解措施	判定通用服务器和数据库为高风险
3998	多项选择题	通常可以从以下哪些方面来确定网络和通信安全层面的测评对象（ ）。	通信主体	网络类型	网络协议	通信模式
3999	多项选择题	通过通信主体来确定网络和通信安全层面的测评对象时，以下关于通信主体的描述，正确的是（ ）。	参与通信的各方，典型的如客户端与服务端	PC机上运行的浏览器与服务器上运行的web服务系统	移动智能终端上运行的APP与服务器上运行的应用系统	服务端与服务端，例如，IPSec VPN与IPSec VPN之间
4000	多项选择题	某网上银行系统通过互联网向其用户提供各种金融服务，用户通过PC端安全浏览器或网银APP进行访问，数据中心部署了SSL VPN网关和应用服务器，以下属于在网络和通信安全层面的测评对象的是（ ）。	安全浏览器和SSL VPN 网关	SSL VPN网关与应用服务器建立的通信信道	安全浏览器与SSL VPN网关建立的通信信道	网银APP与SSL VPN网关建立的通信信道
4001	多项选择题	网络和通信安全层面的通信主体一般包括哪些（ ）。	浏览器与web服务端	APP与后台服务端	IPSecVPN与IPSecVPN	浏览器与SSL VPN

4002	多项选择题	某信息系统包括前台应用系统和后台管理系统，通过互联网或企业内网使用浏览器访问前台应用系统，则网络和通信安全层面的测评对象有哪些（）。	互联网浏览器与前台应用系统之间的通信信道	互联网浏览器与后台管理系统之间的通信信道	企业内网浏览器与前台应用系统之间的通信信道	企业内网浏览器与后台管理系统之间的通信信道
4003	多项选择题	某信息系统包括前台应用系统和后台管理系统，通过非国密浏览器或国密浏览器访问前台应用系统，则网络和通信安全层面的测评对象有哪些（）。	互联网国密浏览器与前台应用系统之间的通信信道	互联网国密浏览器与后台管理系统之间的通信信道	互联网非国密浏览器与前台应用系统之间的通信信道	互联网非国密浏览器与后台管理系统之间的通信信道
4004	多项选择题	某互联网端汽车租赁系统采用B/S架构，通过互联网使用了第三方电子认证服务，则网络和通信安全层面的测评对象有哪些（）。	互联网浏览器与汽车租赁系统之间的通信信道	汽车租赁系统与与第三方电子认证服务相关系统之间的通信信道	互联网浏览器与第三方电子认证服务相关系统之间的通信信道	以上均是
4005	多项选择题	某办公系统部署了SSL VPN安全网关，并向相关用户配发USBKey，实现对PC端登录系统用户的身份鉴别，在密评时以下选项中属于应用和数据安全层面测评对象的是（）。	SSL VPN安全网关	USBKey	PC端浏览器	办公系统
4006	多项选择题	某办公系统部署了SSL VPN安全网关，并向相关用户配发USBKey，实现对PC端登录系统用户的身份鉴别，在密评时以下选项中属于网络和通信安全层面测评对象的是（）。	SSL VPN安全网关	USBKey	PC端浏览器	PC端浏览器与SSL VPN 安全网关之间通信信道
4007	多项选择题	某信息系统的机房和办公区在同一个办公楼且系统和办公区同属于一个网络（办公内网），运维时，可以在办公区通过堡垒机进行设备的运维管理，也可以从互联网和政务外网通过SSL VPN进入办公内网再登录堡垒机运维，则在网络和通信安全层面，以下属于该远程运维管理通道测评对象的是（）。	从互联网访问SSL VPN的通信信道	从政务外网访问SSL VPN的通信信道	从办公网访问堡垒机的通信信道	堡垒机登录设备运维的通信信道

4008	多项选择题	如果被测系统通过统一身份认证系统进行身份鉴别，统一身份认证系统与被测系统不在同一个机房，则“网络和通信安全”层面的测评对象应该包括（ ）。	用户访问被测系统的通信信道	用户访问统一身份认证系统的通信信道	被测系统与统一身份认证系统之间的通信信道	统一身份认证系统本地运维通道
4009	多项选择题	物理和环境安全层面的测评对象为被测信息系统所在的物理机房，具体为（ ）。	物理机房的门禁系统	物理机房的视频监控系统	物理机房的动力环境系统	物理机房的巡查记录
4010	多项选择题	GM/T 0115《信息系统密码应用测评要求》中，应用和数据安全层面的测评对象为“业务应用以及重要数据”，实际测评时，以下表述正确的是（ ）。	应用和数据安全层面的测评对象应包含关键业务应用，具体参考通过专家评审后的密码应用方案设定的范围确定	如无密码应用方案，应根据网络安全等级保护定级报告描述的范围确定	关键业务应用一般情况下应包含被测系统的所有业务应用	关键业务应用中的关键数据一般包含但不限于以下数据：鉴别数据、重要业务数据、重要审计数据、个人敏感信息以及法律法规规定的其他重要数据类型
4011	多项选择题	在针对应用和数据安全层面进行测评时，以下属于该安全层面测评对象的是（ ）。	应用系统管理员	应用系统	密码产品	技术文档
4012	多项选择题	以下可能属于应用和数据安全层面不可否认性测评单元测评时需要关注的内容是（ ）。	接收到重要邮件的确认操作	对重要数据进行签名	公文管理系统业务用户公文签发操作	某银行网上的取钱或转账操作
4013	多项选择题	以下选项中属于业务系统应用和数据安全层面身份鉴别测评单元测评时需要关注的内容是（ ）。	应用系统的业务用户	应用系统的系统管理员用户	应用系统的未注册用户	设备管理员用户
4014	多项选择题	以下可纳入业务系统应用和数据安全层面重要数据存储机密性测评单元测评时需要关注的内容（ ）。	用户名和口令	重要审计数据	公开网站的网站信息	数据库的应用日志记录
4015	多项选择题	以下选项中可纳入业务系统应用和数据安全层面重要数据存储完整性测评单元测评对象的有（ ）。	用户名和口令	重要审计数据	公开网站用户浏览记录	数据库的应用日志记录
4016	多项选择题	业务应用中的关键数据一般包含但不限于以下数据（ ）。	鉴别数据	重要审计数据	个人敏感信息	需备份的密钥

4017	多项选择题	使用密码技术的加解密功能实现机密性，信息系统中保护的对象一般包括（ ）。	身份鉴别信息	公钥数据	传输的重要数据	信息系统应用中存储的重要数据
4018	判断题	某信息系统部署在公有云平台上，云平台所在机房未开展过商用密码应用安全性评估，在对该系统开展密评时，密评人员需到云平台所在机房现场进行取证。	正确	错误		
4019	判断题	根据《商用密码应用安全性评估FAQ（第二版）》，交换机、网闸、防火墙、WAF等未使用密码功能的网络设备、安全设备一般不作为设备和计算安全层面的测评对象。	正确	错误		
4020	判断题	根据《商用密码应用安全性评估FAQ（第二版）》，对信息系统进行测评时，若存在设备管理通道跨越网络边界的情况，需在网络和通信安全层面梳理相应的远程管理数据传输通道作为测评对象。	正确	错误		
4021	判断题	根据《商用密码应用安全性评估FAQ（第二版）》，对信息系统进行测评时，针对通用服务器，以“具有相同硬件、软件配置的设备”为粒度确定测评对象，即具有相同硬件配置（如生产厂商、型号等）和软件配置（如操作系统版本、中间件等）的服务器作为一个测评对象。	正确	错误		
4022	判断题	若系统未部署SSL VPN，管理员通过互联网直接访问堡垒机对设备进行管理，在设备和计算安全层面“远程管理通道安全”测评单元可将访问堡垒机的信息传输通道作为测评对象。	正确	错误		
4023	判断题	针对通用服务器，以“具有相同硬件、软件配置的设备”为粒度确定测评对象。	正确	错误		

4024	判断题	根据《商用密码应用安全性评估FAQ（第二版）》，某信息系统部署了5台生产厂商为型号为操作系统版本为C的应用服务器，则在密评时需抽选任意2台应用服务器作为设备和计算安全层面的测评对象。	正确	错误		
4025	判断题	管理员在互联网通过SSL VPN接入系统内网，登录堡垒机后采用SSH协议对设备进行远程管理，针对设备和计算安全层面的“远程管理通道安全”测评单元，应将管理员在互联网通过VPN接入系统内网的过程进行测评。	正确	错误		
4026	判断题	根据《商用密码应用安全性评估FAQ（第二版）》，应用和数据安全层面的测评对象为关键业务应用，关键业务应用一般情况下应包含被测系统的所有业务应用。	正确	错误		
4027	判断题	某信息系统中通过堡垒机对设备进行远程运维，则设备和计算安全层的远程管理通信安全的测评对象不包括堡垒机。	正确	错误		
4028	判断题	根据《商用密码应用安全性评估FAQ（第二版）》，某三级信息系统部署了经检测认证合格的服务器密码机（密码模块为二级），则密评时针对设备和计算安全层面“系统资源访问控制信息完整性”指标要求，该服务器密码机可直接判定为符合。	正确	错误		
4029	判断题	根据《商用密码应用安全性评估FAQ（第二版）》，可根据网络类型来确定网络和通信安全层面的测评对象。	正确	错误		

4030	判断题	根据《商用密码应用安全性评估FAQ（第二版）》，网络和通信安全层面的测评对象的选择，只需区分系统所属的网络环境是内网还是外网即可确定测评对象。	正确	错误		
4031	判断题	若信息系统在网络边界未部署SSL VPN，管理员通过互联网直接访问堡垒机对设备进行管理，在网络和通信安全层面“通信数据完整性”测评单元应将访问堡垒机的信息传输通道作为测评对象。	正确	错误		
4032	判断题	根据《商用密码应用安全性评估FAQ（第二版）》，网络和通信安全层面的测评对象主要是跨网络访问的通信信道。	正确	错误		
4033	判断题	某等保四级办公系统为独立的内网系统，且不允许跨网络边界进行远程运维，则整个网络和通信安全层面一定作为不适用处理。	正确	错误		
4034	判断题	某信息系统部署在公有云平台的独立VPC内，通过云平台的堡垒机对设备进行远程管理，应将堡垒机与设备之间的远程管理通道作为网络和通信安全层面的测评对象。	正确	错误		
4035	判断题	如果被测信息系统所在的物理机房采用多区域部署时，密评人员在测评时只需到个别机房进行现场取证。	正确	错误		
4036	判断题	如果被测信息系统部署在被测单位管辖范围之外，物理和环境安全层面的测评指标通常为适用。	正确	错误		
4037	判断题	如果被测信息系统所在的IDC机房通过了密评，则可以复用密评报告中“物理和环境安全”层面的相关测评结论。	正确	错误		

4038	判断题	某三级信息系统部署在公有云平台上，由云服务提供商负责机房环境管理，在对该系统开展密评时，物理和环境安全层面一定作为不适用处理。	正确	错误		
4039	判断题	某三级信息系统部署在办公大楼的机房里，机房和办公大楼都部署有电子门禁系统，则仅需将机房的电子门禁系统纳入测评范围。	正确	错误		
4040	判断题	某三级信息系统部署在办公大楼的机房里，机房和办公大楼都部署有视频监控系统，则办公大楼和机房的视频监控系统一定纳入测评。	正确	错误		
4041	判断题	如果被测信息系统所在的IDC机房、运营商机房或云服务提供商机房等未开展密评，测评时，密评人员也需现场取证，对其进行测评。	正确	错误		
4042	判断题	根据《商用密码应用安全性评估FAQ（第二版）》，在对云平台进行密评时，云平台密码资源池的密码管理平台通常作为应用和数据安全层面的测评对象。	正确	错误		
4043	判断题	《商用密码应用安全性评估FAQ（第二版）》中，关于云平台测评提及的被部分评估的支撑能力，指的是云平台提供的某些支撑服务，这些支撑服务仅用于云上应用而不用于云平台，或者将服务于云平台和云上应用的不同测评对象。	正确	错误		
4044	判断题	根据《商用密码应用安全性评估FAQ（第二版）》，云平台运行所在的机房同时支撑了云平台和云上应用在物理和环境安全层面的密码应用安全，将在云平台密码应用安全性评估时被“完全评估”。	正确	错误		

4045	判断题	根据《商用密码应用安全性评估FAQ（第二版）》，被“完全评估”表明该支撑能力有明确的测评结果（包括量化评估、风险评价等）	正确	错误		
4046	判断题	根据《商用密码应用安全性评估FAQ（第二版）》，如果云平台的电子签章系统仅用于支撑了云上应用进行合同签署，实现抗抵赖保护，而不用于云平台本身，则电子签章服务属于被部分评估的支撑能力。	正确	错误		
4047	判断题	根据《商用密码应用安全性评估FAQ（第二版）》，云服务器密码机在进行数据存储保护时，面向的是云平台和云上应用的不同数据。此时，该支撑能力在云平台测评时进行“完全评估”。	正确	错误		
4048	判断题	根据《商用密码应用安全性评估FAQ（第二版）》，云上应用密评时，只关注应用本身在各个安全层面的密码应用情况。	正确	错误		
4049	判断题	某一信息系统通过统一身份认证系统进行身份鉴别，统一身份认证系统未开展密评，则该信息系统测评时应把统一身份认证系统纳入测评范围。	正确	错误		
4050	单项选择题	根据（ ）测评指标的要求，测评实施时，需要查看信息系统责任单位是否制定了管理制度发布的相关要求。	应明确相关管理制度的发布流程	制度执行过程应留存相关执行记录	定期对存在不足或需要改进的安全管理制度进行修订	应制定密码安全管理制度及操作规范
4051	单项选择题	在第四级信息系统的安全管理测评中，需要对密钥管理员、密码产品操作人员实施必要的审查，具体是指（ ）。	在人员录用时对录用人员执业资质、社会关系等进行审查	在人员录用时对录用人员家庭背景、犯罪记录和亲属等进行审查	在人员录用时对录用人员政治面貌、亲属关系等进行审查	在人员录用时对录用人员身份、背景、专业资格和资质等进行审查

4052	单项选择题	某三级信息系统只能在机房通过堡垒机对服务器进行运维管理，则设备和计算安全层面堡垒机、服务器关于“远程管理通道安全”测评指标的适用性分别为（ ）。	不适用，不适用	不适用，适用	适用，不适用	适用，适用
4053	单项选择题	某二级信息系统责任单位认为，该系统某条通信信道的通信机密性和通信完整性难以通过密码技术实现，并在密码应用方案中明确说明了该两个指标作为不适用项，则密码应用方案编制时（ ）。	明确说明通信机密性和机密性的不适用情况和原因，并对两个指标采用相应的风险控制措施	明确说明通信机密性和机密性的不适用情况和原因，并对通信机密性指标采用相应的风险控制措施	明确说明通信机密性和机密性的不适用情况和原因性，并对通信完整性指标采用相应的风险控制措施	明确说明通信机密性和机密性的不适用情况和原因，两个指标都无需采用风险控制措施
4054	单项选择题	某二级信息系统责任单位认为，该系统某条通信信道的通信机密性和通信完整性无需实现，并在密码应用方案明确说明了该指标的不适用性，则以下表述更为合理的是（ ）。	密评人员在测评时，可考虑把两个指标不纳入测评范围，但通信信道的通信机密性需核实风险控制措施的适用条件	密评人员在测评时，可考虑把两个指标不纳入测评范围，但通信信道的通信完整性需核实风险控制措施的适用条件	密评人员在测评时，可考虑把两个指标不纳入测评范围，两个指标都要核实风险控制措施的适用条件	密评人员在测评时，可考虑把两个指标直接不纳入测评范围
4055	单项选择题	某三级信息系统责任单位认为该系统在“网络和通信安全”层面无安全接入认证需求，并在密码应用方案明确说明了该指标的不适用原因，则（ ）。	密评人员在测评时，可考虑把该指标直接不纳入测评范围	密评人员在测评时，可考虑把该指标不纳入测评范围，但需核实风险控制措施的适用条件	密评人员在测评时，可不考虑密码应用方案，直接把该指标纳入测评范围，并判为不符合	密评人员在测评时，可不考虑密码应用方案，直接把该指标纳入测评范围，并根据实际情况测评
4056	单项选择题	某二级信息系统责任单位不计划把电子门禁记录数据存储完整性指标纳入测评范围，则应在设计密码应用方案时（ ）。	不需要明确说明电子门禁记录数据存储完整性指标的不适用性	需要明确说明电子门禁记录数据存储完整性指标的不适用性，但不需要采取风险控制措施	需要明确说明电子门禁记录数据存储完整性指标的不适用性，并且需要采取风险控制措施	无法作为不适用项

4057	单项选择题	某二级信息系统责任单位不计划把视频监控记录数据存储完整性指标纳入测评范围，在设计密码应用方案时（ ）。	不需要明确说明视频监控记录数据存储完整性指标的不适用性	需要明确说明视频监控记录数据存储完整性指标的不适用性，但不需要采取风险控制措施	需要明确说明视频监控记录数据存储完整性指标的不适用性，并且需要采取风险控制措施	视频监控记录数据存储完整性指标无法作为不适用项
4058	多项选择题	以下哪几项是存在缺陷或有安全问题警示的密码技术（ ）。	SSH 1.0	SSL 2.0	TLS 1.3	SSL 3.0
4059	多项选择题	设备和计算安全层面，如果信息系统通过堡垒机统一运维管理设备，而堡垒机前部署了合规的SSL VPN，以下哪些表述正确（ ）。	VPN 解决的是远程管理通道的安全问题	VPN不能解决堡垒机与其他被运维设备的身份鉴别	堡垒机与被运维设备的身份鉴别应各自独立进行判定	未使用密码技术进行身份鉴别的堡垒机可以不作为测评对象
4060	多项选择题	管理员在本地进行应用服务器登录运维，且应用服务器部署在相对安全的机房内部，在设备和计算安全层面，哪些测评指标应作为适用项（ ）。	身份鉴别	远程管理通道安全	系统资源访问控制信息完整性	日志记录完整性
4061	判断题	根据《商用密码应用安全性评估FAQ（第二版）》，系统2019年12月27日投入运行，首次测评时，建设运行方面“投入运行前进行密码应用安全性评估”测评项可判定为不适用。	正确	错误		
4062	判断题	根据《商用密码应用安全性评估FAQ（第二版）》，系统2019年12月27日投入运行，首次测评不通过，改造后在对信息系统进行复评时，建设运行方面“投入运行前进行密码应用安全性评估”测评项可判定不适用。	正确	错误		
4063	判断题	某三级信息系统进行密评时，经访谈运维人员后得知，本系统从未发生安全事件，但有应急处置相关管理制度。因此，应急处置方面的向有关主管部门上报处置情况指标为不适用。	正确	错误		

4064	判断题	在对设备和计算安全层面“身份鉴别”测评指标进行测评时，若运维管理员均未采用密码技术对登录设备的用户进行身份鉴别，则该测评对象的测评结果为不符合。	正确	错误		
4065	判断题	管理员在本地进行应用服务器登录运维，且应用服务器部署在屏蔽机房内，经核查发现应用服务器关闭了远程运维接口，则针对应用服务器的“远程管理通道安全”测评指标可作为不适用项。	正确	错误		
4066	判断题	经测评发现，某信息系统中所有设备设置不涉及重要信息资源安全标记，测评人员则对设备和计算安全层面的重要信息资源安全标记完整性测评单元判定结果为不符合。	正确	错误		
4067	判断题	在对应用用户的应用和数据安全层面“身份鉴别”测评指标进行测评时，若实现用户身份真实性所采用的密码使用不正确或无效，则该测评对象的测评结果为不符合。	正确	错误		
4068	单项选择题	某信息系统于2018年投入运行，该系统首次密码应用安全性评估时在建设运行层面“投入运行前进行密码应用安全性评估”测评项应如何判定（ ）。	判定“不符合”	判定“符合”	判定“不适用”	判定“部分符合”
4069	单项选择题	某信息系统于2022年投入运行，该系统首次密码应用安全性评估时在建设运行层面“投入运行前进行密码应用安全性评估”测评项应如何判定（ ）。	判定“不符合”	判定“符合”	判定“不适用”	判定“部分符合”
4070	单项选择题	某信息系统于2021年投入运行，同年开展了商用密码应用安全性评估，则再次开展密码应用安全性评估时在建设运行层面“投入运行前进行密码应用安全性评估”测评项应如何判定（ ）。	判定“不符合”	判定“符合”	判定“不适用”	判定“部分符合”

4071	单项选择题	以下哪些密码产品适用于GM/T0028《密码模块安全技术要求》（）。	服务器密码机	安全芯片	CA/KM系统	电子签章系统
4072	单项选择题	对通过工具测试抓取的数据进行分析，下列哪些说法是不正确的（ ）。	对密文应进行随机性检测	查看关键字段是否以明文出现	验证杂凑值和签名值是否正确	对密文进行解密，验证加密算法的合规性、正确性
4073	单项选择题	经核查，某信息系统通过调用服务器密码机，对系统日志记录进行完整性保护，防止日志记录被非法篡改，则建议配置的密码算法为（ ）。	HMAC-MD5	HMAC-SM3	HMAC-SHA1	SM4
4074	单项选择题	某信息系统部署了1台经检测认证合格的SSL VPN，则在设备和计算安全层面，关于该SSL VPN，哪些指标不能直接判定为符合（ ）。	身份鉴别	系统资源访问控制信息完整性	日志记录完整性	重要可执行程序完整性
4075	单项选择题	某三级信息系统部署了经检测认证合格的安全认证网关（密码模块二级）实现网络通信传输保护，但该系统客户端浏览器仅支持国外密码算法，则针对网络和通信安全层面的通信过程的机密性和网络边界访问控制信息完整性两个指标的判定为（ ）。	都为部分符合	前者为部分符合，后者为符合	前者为符合，后者为部分符合	前者为部分符合，后者为不符合
4076	单项选择题	某电商平台收集了用户的姓名、手机号、地址等信息，需要对这些信息进行存储完整性保护，则应采取的密码技术为（ ）。	SM3	HMAC-SM3	MD5	SM4
4077	单项选择题	某信息系统需要采用密码技术实现数据原发行为和接收行为的不可否认性，则应采取的密码技术为（ ）。	SM3	AES	SM4	SM2签名算法
4078	单项选择题	某信息系统部署了1台经检测认证合格的SSL VPN安全网关，管理员在互联网通过该SSL VPN安全网关接入系统，经抓包分析发现，使用的密码算法套件为ECC_SM4_SM3，则应用和数据安全层面“重要数据传输机密性”测评单元应判定为（ ）。	符合	部分符合	不符合	不适用

4079	单项选择题	某三级信息系统部署在云平台上，则承载该信息系统的云平台的安全保护等级不低于第（ ）级。	一	二	三	四
4080	单项选择题	对于数据库中的重要业务数据存储完整性保护，使用SM3算法进行保护，判定为（ ）。	符合	部分符合	不符合	采取了风险缓解措施
4081	单项选择题	信息系统用户登录口令通过加盐的杂凑算法运算后存储在数据库中，系统本身不存储原始口令，则该系统对口令存储实现了（ ）保护。	真实性	机密性	完整性	不可否认性
4082	单项选择题	在密评实施过程中，发现用户虽然使用HMAC-SM3对口令数据进行完整性保护，且采用认证合格的智能密码钥匙生成MAC，但是只截取使用了MAC值的前8个比特，那么对应用和数据安全层面的“重要数据存储完整性保护”指标判定时，以下DAK判定最为合理的是（ ）。	√√√	√××	√√×	×√√
4083	单项选择题	在密评实施过程中，发现系统对口令进行了SM3杂凑计算对其传输和存储进行了保护，且采用认证合格的智能密码钥匙生成MAC，那么对应用和数据安全层面的“身份鉴别”指标判定时，以下DAK判定最为合理的是（ ）。	√√√	√××	√√×	×√√
4084	单项选择题	信息系统使用的密码算法如果不是以国家标准或行业标准发布的，在测评时首先应核验（ ）。	是否取得国家密码管理部门同意其使用的证明文件	密码算法安全性审查文件	密码算法正确性验证报告	密码算法性能测试报告
4085	单项选择题	某信息系统的网络安全保护等级为S3A2，则对该信息系统进行密评时，则应从GB/T 39786《信息安全技术 信息系统密码应用基本要求》中选择第（ ）级指标要求作为测评指标。	一	二	三	四

4086	单项选择题	在对某地级市门户网站系统进行密码应用安全性评估时，发现该系统未完成网络安全等级保护定级备案，则通常应按照GB/T 39786第几级密码应用基本要求进行测评（ ）。	一	二	三	四
4087	多项选择题	以下关于密评中针对服务器密码机的测评方法描述，合理的是（ ）。	利用Wireshark，抓取应用系统调用密码机的指令报文，验证调用频率是否正常	利用Wireshark，抓取应用系统调用密码机的指令报文，验证调用指令是否正确	管理员登录密码机查看相关配置，检查内部存储的密钥是否对应合规的密码算法	管理员登录密码机查看相关日志文件，根据与密钥管理、密码计算相关的日志记录，检查是否使用合规的密码算法
4088	多项选择题	以下哪些密码产品不适用于GM/T 0028《密码模块安全技术要求》（ ）。	服务器密码机	安全芯片	CA/KM系统	电子签章系统
4089	多项选择题	某三级信息系统部署了1台商用密码产品认证证书编号均为GMxxx的SSL VPN，则针对“密码产品合规性”测评内容主要包括（ ）。	核查该密码产品型号、版本等信息是否与证书一致	核查该密码产品的使用是否满足其安全运行的条件	核查该密码产品的密码模块安全等级是否满足要求	核查密码产品是否对登录用户进行身份鉴别
4090	多项选择题	以下选项属于设备和计算安全层面访问控制信息的是（ ）。	操作系统权限的访问控制信息	系统文件目录的访问控制信息	防火墙（不含密码功能）的访问控制列表	堡垒机中的权限访问控制信息
4091	多项选择题	对于设备和计算安全层面“重要信息资源安全标记完整性”，测评单位在测评实施时主要实施以下哪些内容（ ）。	查看技术文档中重要信息资源安全标记完整性保护所采用的密码技术及实现机制	核验并验证系统中重要信息资源安全标记完整性保护的正确性	核验系统中重要信息资源安全标记完整性保护的有效性	核查重要信息资源安全标记完整性保护使用的密码算法是否符合密码相关国家标准和行业标准
4092	多项选择题	某三级信息系统中使用动态令牌系统实现管理员登录堡垒机的身份鉴别，则关于设备和计算安全层面堡垒机身份鉴别的测评方法包括（ ）。	核查动态令牌系统是否为经检测认证合格的商用密码产品	核查动态令牌系统配置（算法、协议等）是否正确	核查堡垒机使用动态令牌实现身份鉴别所使用的密码算法的合规性	核查动态令牌密码模块安全等级是否为二级

4093	多项选择题	在网络和通信安全层面，访问控制信息可能包括以下选项中的（）。	VPN设备中的访问控制列表	堡垒机中的访问控制列表	防火墙的访问控制列表	边界路由的访问控制列表
4094	多项选择题	在设备和计算安全层面，访问控制信息主要包括（ ）。	操作系统权限的访问控制信息	系统文件目录的访问控制信息	数据库中的数据访问控制信息	堡垒机中的权限访问控制信息
4095	多项选择题	经核查，某信息系统PC端安全浏览器与SSL VPN安全网关之间使用了合规的SSL协议，安全浏览器和SSL VPN安全网关均具有有效期内的认证证书，且密码模块等级符合要求，在网络和通信安全层面哪些测评单元可以判定为符合（）。	身份鉴别	通信数据完整性	通信过程中重要数据的机密性	安全接入认证
4096	多项选择题	某信息系统部署了安全认证网关代理应用系统，用户通过智能密码钥匙访问应用系统，下列哪些属于该访问应用通信信道身份鉴别测评单元的测评方法（）。	核查安全认证网关的商用密码产品认证证书	核查智能密码钥匙的商用密码产品认证证书	通过抓包核查通信过程中的握手协议	通过抓包核查通信过程中的记录协议
4097	多项选择题	某网站用户需要通过浏览器采用HTTPS协议进行访问，下列哪些属于该访问网站通信信道身份鉴别测评单元可能涉及到的测评内容（）。	核查服务端是否采用了合规的商用密码产品	核查网站站点证书的证书链	通过抓包分析其通信协议中对服务端的身份鉴别方法	核查通信协议中数据传输加密使用的算法
4098	多项选择题	某信息系统部署了SSL VPN对设备运维进行保护，系统也部署了防火墙进行网络访问控制，则该运维通信信道的网络边界访问控制信息测评单元的测评方法包括（）。	核查SSL VPN的商用密码产品认证证书	如果SSL VPN合规，则无需核查网络边界访问控制信息完整性的密码实现技术	如果SSL VPN不合规，则需核查网络边界访问控制信息完整性的密码实现技术	核查防火墙的商用密码产品认证证书
4099	多项选择题	某单位数据中心机房出入口安装了电子门禁系统，则针对“电子门禁记录数据存储完整性”测评单元，主要测评内容包括（）。	核查是否采用了经检测认证的电子门禁系统	核查是否正确使用经检测认证的电子门禁系统	核查门禁系统厂商提供的门禁系统进出记录数据存储完整性保护的相关证据	验证完整性保护机制是否正确和有效

4100	多项选择题	某信息系统所在机房部署了电子门禁系统进行物理访问身份鉴别，经核查发现电子门禁系统基于指纹对人员进行身份鉴别，则物理和环境安全层面“身份鉴别”测评单元如何判定，风险等级如何变化（ ）。	符合	不符合	风险等级降低	风险等级不变
4101	多项选择题	某机房部署了电子门禁系统，以下哪些属于电子门禁系统身份鉴别测评单元的测评方法（ ）。	查看发卡时密钥分散的密码算法	核查电子门禁系统的商用密码产品认证证书	核查门禁卡的管理制度	核查是否有机房进出登记记录
4102	多项选择题	某机房电子门禁记录数据完整性保护通过服务器密码机的HMAC实现，以下哪些属于电子门禁记录数据存储完整性测评单元的测评方法（ ）。	核查电子门禁系统的商用密码产品认证证书	核查服务器密码机的商用密码产品认证证书	核查是否能够修改电子门禁记录	核查是否能够发现修改电子门禁记录数据
4103	多项选择题	某机房部署了视频监控系统，数据影像记录存储在加密存储系统中，以下哪些不属于视频监控记录数据存储完整性测评单元的测评方法（ ）。	核查视频监控系统的商用密码产品认证证书	核查加密存储系统的商用密码产品认证证书	核查视频监控系统视频传输的密码实现	核查摄像头终端的视频传输密码实现
4104	多项选择题	某电商平台收集了用户的姓名、手机号、地址等信息，需要对这些信息进行存储完整性保护，可采用的完整性保护机制包括（ ）。	SM3	HMAC-SM3	HMAC-SM4	SM2签名算法
4105	多项选择题	某信息系统采用动态口令机制对登录用户进行身份鉴别，针对应用和数据安全层面“身份鉴别”测评单元，应核查的内容包括（ ）。	核查密码算法合规性	核查密码技术合规性	核查密码产品合规性	核查动态口令机制是否正确和有效
4106	多项选择题	某信息系统拟采用密码技术对登录用户进行身份鉴别，可以使用的密码技术包括（ ）。	采用动态口令机制	基于对称密码算法的消息鉴别码机制	基于密码杂凑算法的消息鉴别码机制	基于公钥密码算法的数字签名机制
4107	多项选择题	某信息系统拟采用密码技术对保证应用的访问控制信息的完整性，可以使用的密码技术包括（ ）。	采用动态口令机制	基于对称密码算法的消息鉴别码机制	基于密码杂凑算法的消息鉴别码机制	基于公钥密码算法的数字签名机制

4108	多项选择题	某云平台部署了服务器密码机对云平台和云上应用提供数据存储保护，部署了电子签章系统供云上应用调用，该云平台未通过密码应用安全性评估，则针对云上应用进行密码应用安全性评估时，以下描述合理的是（ ）。	云平台运行所在机房应作为测评对象	云平台运行所在机房不作为测评对象	服务器密码机应作为测评对象	电子签章系统应作为测评对象
4109	多项选择题	某公有云平台部署了服务器密码机对云平台和云上应用提供数据存储保护，部署了电子签章系统仅供云上应用调用，则在对公有云平台进行密码应用安全性评估时，以下关于测评对象选择正确的是（ ）。	云平台运行所在机房应作为测评对象	服务器密码机不作为测评对象	服务器密码机应作为测评对象	电子签章系统应作为测评对象
4110	多项选择题	某云平台部署了服务器密码机，同时面向云平台和云上应用提供数据存储保护，且云平台已经通过了密码应用安全性评估，在对云上应用进行密码应用安全性评估时，以下描述正确的是（ ）。	服务器密码机不作为测评对象	服务器密码机应作为测评对象	直接引用云平台的服务器密码机测评结果	服务器密码机应结合业务应用一起测评
4111	多项选择题	信息系统通过调用合规的云服务器密码机对重要数据使用SM4-GCM进行保护，以下关于测评工作的描述，正确的是（ ）。	需要核查是否实现重要数据的机密性保护	需要核查是否实现重要数据的完整性保护	需要核查云服务器密码机的商用密码产品认证证书	由于云服务器密码机由运营商负责，因此无需核查其合规性
4112	多项选择题	对于更换商用密码产品认证证书的密码产品，如果未标注密码模块安全等级，以下描述正确的是（ ）。	需要进一步提供换证前的商用密码产品型号证书	需要确认换证前的商用密码产品型号证书的安全等级是否符合要求	未提供安全等级证明的按照“密码产品符合一级密码模块”进行判定	提供密码产品的密钥管理方案，证明其符合安全要求，并按“密码产品等级符合”判定

4113	多项选择题	密码产品核查是测评过程的重点，测评时需要核查以下哪些方面（ ）。	确认所有实现的密码算法、密码协议是否获得了商密检测机构出具的合格检测报告或密码产品是否获得了商用密码产品认证证书	评估密码产品是否被正确、有效使用	已经检测认证合格的产品，是否使用了未经认可的密码算法或协议	密码产品是否被错误使用、配置，甚至被旁路
4114	多项选择题	以下针对云平台开展测评工作的描述，表述合理的是（ ）。	云平台测评与一般信息系统涉及的测评指标基本一致	应关注云平台自身的密码应用以及对云租户提供的密码服务	对于云平台自身而言，要分别对云平台支持的每类服务模式（IaaS、PaaS、SaaS）进行密码应用测评	应关注对云租户提供的密码服务都有哪些，每台 密码设备服务的边界
4115	多项选择题	某信息系统在密码应用方案中明确了需要对注册用户的手机号进行机密性保护，可以采用的密码算法包括（ ）。	DES	SM2	SM3	SM4
4116	多项选择题	判断B用户拥有的数字证书是否是CA机构A签发的，需要执行的操作是（ ）。	查看B用户证书中颁发者信息和颁发者密钥标识符是否与A机构CA证书中的主体名称信息和主体密钥标识符一致	查看B用户证书中主体名称信息和主体密钥标识符是否与A机构CA证书中的主体名称信息和主体密钥标识符一致	使用A机构CA证书的公钥，验证B用户证书的签名值是否正确	查看B用户证书中主体名称信息和A机构CA证书的颁发者信息是否一致
4117	判断题	对2020年1月1日以后建设运行的信息系统，由于在系统规划时未制定密码应用方案，因此在密评时“制定密码应用方案”测评指标可判定为“不适用”。	正确	错误		

4118	判断题	某三级信息系统部署了1台经检测认证合格的SSL VPN，经核查其产品认证证书，发现证书未标注密码模块安全等级（非换证密码产品），则该SSL VPN应按“密码产品符合一级密码模块”进行判定。	正确	错误		
4119	判断题	经核查，某三级信息系统通过调用经检测认证合格的服务器密码机（密码模块二级），使用HMAC-SM3对应用日志记录进行存储完整性保护，则应用和数据安全层面针对日志记录完整性保护可判定为符合。	正确	错误		
4120	判断题	在进行密评时，如果信息系统网络安全等级保护定级为四级，但密码应用方案按照信息系统密码应用等级三级进行评审，则可按照信息系统密码应用安全等级三级进行测评。	正确	错误		
4121	判断题	根据《商用密码应用安全性评估FAQ（第二版）》，某三级信息系统部署了1台经检测认证合格的SSL VPN（密码模块二级），则在设备和计算安全层面，针对该SSL VPN的“身份鉴别”测评指标可直接判定为符合。	正确	错误		
4122	判断题	根据《商用密码应用安全性评估FAQ（第二版）》，某三级信息系统部署了1台经检测认证合格的SSL VPN（二级密码模块），则在设备和计算安全层面，针对该SSL VPN的“系统资源访问控制信息完整性”“日志记录完整性”测评指标可直接判定为符合。	正确	错误		

4123	判断题	某信息系统使用堡垒机对设备进行统一管理，堡垒机使用了合规的智能密码钥匙实现身份鉴别，则针对统一管理的所有设备的“身份鉴别”指标即可判定为“符合”。	正确	错误		
4124	判断题	某信息系统所在机房部署了电子门禁系统进行人员进入机房时的身份鉴别，经核查发现电子门禁系统基于指纹对人员进行身份鉴别，则物理和环境安全层面“身份鉴别”测评单元可判定为符合。	正确	错误		
4125	判断题	某机房的电子门禁系统通过MIFARE卡进行身份鉴别，则该电子门禁系统的身份鉴别通常判定为符合。	正确	错误		
4126	判断题	某机房的电子门禁系统通过ID卡进行身份鉴别，则该电子门禁系统的身份鉴别通常判定为部分符合。	正确	错误		
4127	判断题	某机房的电子门禁系统通过指纹进行身份鉴别，则该电子门禁系统的身份鉴别通常应判定为不符合。	正确	错误		
4128	判断题	根据《商用密码应用安全性评估FAQ（第二版）》，云平台通过密评（即密评结论为“符合”或“基本符合”），但是当云平台自身密码应用安全等级低于云上应用时，在对云上应用测评时，云平台的“云平台支撑能力说明”不再有效，仍需要对云平台相关的密码应用进行重新测评。	正确	错误		
4129	判断题	根据《商用密码应用安全性评估FAQ（第二版）》，云平台未通过密评（未开展密评，或密评结论为“不符合”）时，在对云上应用测评时，仍需要对云平台相关的密码应用进行（重新）测评。	正确	错误		

4130	判断题	某信息系统使用SM3算法对数据库中的重要数据存储进行完整性保护，则“重要数据存储完整性”的测评单元判定为符合。	正确	错误		
4131	判断题	某信息系统采用动态口令机制对登录应用用户进行身份鉴别，则在应用和数据安全层面“身份鉴别”测评单元的判定结果一定为“符合”。	正确	错误		
4132	判断题	根据《商用密码应用安全性评估FAQ（第二版）》，通常来说，云上应用系统所处的云平台通过密评后，云上应用系统才能通过密评。	正确	错误		
4133	判断题	某信息系统部署在公有云平台上，该公有云平台已经通过了密评，且该公有云安全等级不低于云上应用，则在对该云上信息系统进行密评时，物理和环境安全层面可作为不适用。	正确	错误		
4134	判断题	根据《商用密码应用安全性评估FAQ（第二版）》，仅为云上应用提供云密码支撑服务的密码资源池的测评不影响云平台最终测评结论。	正确	错误		
4135	判断题	如果云平台未通过密评，则对云上应用测评时，应涉及为云上应用提供密码运算的云服务器密码机实体机的密评。	正确	错误		
4136	判断题	云平台一般会提供一些原始镜像给租户使用，租户启动原始镜像生成自己的虚拟机。云平台测评时，租户的原始镜像通常作为重要可执行程序进行测评。	正确	错误		
4137	判断题	某三级信息系统，使用经检测认证合格的商用密码产品（密码模块二级），根据GM/T 0115《信息系统密码应用测评要求》中“5.5密钥管理安全性”测评指标不能直接判定为“符合”。	正确	错误		

4138	判断题	如果密码产品有商用密码产品认证证书但认证证书已经过期，则相应密码应用的密钥管理安全可判为不符合。	正确	错误		
4139	判断题	若信息系统编制了密码应用方案，且方案通过评估，方案中明确了不适用的“宜”的指标要求项，密码应用安全性评估人员在测评时，该测评指标一定为“不适用”。	正确	错误		
4140	判断题	对于已建并且正在运行的信息系统，其密码应用方案并不追溯到系统最初规划时的方案，制定的密码应用改造方案可视为该系统的密码应用方案。	正确	错误		
4141	判断题	在对信息系统密码应用方案进行密评时，如果所有测评指标项评估结论均为通过，则该信息系统密码应用方案密评结论为通过。	正确	错误		
4142	判断题	某信息系统部署了SSL VPN安全网关，PC端安全浏览器与SSL VPN安全网关之间使用SSL协议建立通信信道，测评时应在PC端安全浏览器与SSL VPN安全网关之间设置抓包点，分析通信信道的安全性。	正确	错误		
4143	判断题	某三级信息系统部署了1台经检测认证合格的SSL VPN安全网关，则关于该SSL VPN的“密钥管理安全性”测评可以直接判定为“符合”。	正确	错误		
4144	判断题	在对某三级信息系统进行密评时，通过对应用系统分析核查，发现系统启用了TLS 1.1、TLS 1.2协议，则关于通用要求中的“密码技术合规性”测评单元可直接判定为符合。	正确	错误		
4145	判断题	某信息系统将登录用户口令进行加密后存储在数据库中，经核查所使用的密码算法为SHA-1，这种口令存储加密保护方式符合要求。	正确	错误		

4146	判断题	某信息系统编制了密码应用方案，且方案通过专家评估，方案中明确了不适用的“宜”的指标要求项，在密评时发现密码应用实施情况与方案中所描述的风险控制措施不一致，则这些指标要求项应纳入测评范围。	正确	错误		
4147	单项选择题	密评过程中，依据（ ）标准进行IPSec协议数据的分析。	GM/T 0022《IPSec VPN技术规范》	GM/T 0023《IPSec VPN网关产品规范》	GM/T 0024《SSL VPN技术规范》	GM/T 0025《SSL VPN网关产品规范》
4148	单项选择题	密评过程中，依据（ ）标准进行SSL协议数据的分析。	GM/T 0022《IPSec VPN技术规范》	GM/T 0023《IPSec VPN网关产品规范》	GM/T 0024《SSL VPN技术规范》	GM/T 0025《SSL VPN网关产品规范》
4149	单项选择题	某信息系统的通用服务器，通过调用服务器密码机进行加解密处理，以下测评方式不合理的是（ ）。	在通用服务器上安装网络抓包分析工具采集交互的数据包	在通用服务器和服务器密码机所在的交换机进行端口镜像进行获取	在服务器密码机上安装网络抓包分析工具采集交互的数据包	登录服务器密码机，查看相关的配置和日志
4150	单项选择题	密评过程中，采用端口扫描主要用于探测和识别被测信息系统中的VPN、服务器密码机、数据库服务器等设备开放的端口服务，如果发现（ ）端口是开放的，一般可以作为SSL VPN服务开启的辅助证据之一。	443	3389	500	22
4151	单项选择题	密评过程中，采用端口扫描主要用于探测和识别被测信息系统中的VPN、服务器密码机、数据库服务器等设备开放的端口服务，如果发现（ ）端口是开放的，可以作为SSH服务开启的证据。	443	3389	500	22
4152	单项选择题	在分析对网络信道中的SSL协议的握手协议时，在（ ）报文之后，相应的数据包会被加密无法进行解析。	Client Key Exchage	Change Cipher Spec	Certificate Verify	Server Hello Done
4153	单项选择题	在密评时，可以根据GM/T 0005针对（ ）检测其随机数统计特性，判断其是否符合要求。	随机数熵源	应用中采集的大量CBC模式下的IV值构成的数据样本	应用中采集的大量CTR模式下的计数器构成的数据样本	数字证书

4154	单项选择题	在使用Wireshark工具时，在工具过滤器中输入（ ）可以用于仅显示源IP地址为192.168.1.100的网络数据包。	ip.addr == 192.168.1.100	ip.src == 192.168.1.100	ip.dst == 192.168.1.100	ip.host == 192.168.1.100
4155	单项选择题	下列Wireshark过滤表达式（ ）可以捕获所有发往或来自IP地址192.168.1.100的HTTP流量。	http.host == 192.168.1.100	ip.addr == 192.168.1.100 && tcp.port == 80	http.request.method == "GET" && ip.addr == 192.168.1.100	http.response.code == 200 && ip.dst == 192.168.1.100
4156	单项选择题	下列Wireshark过滤表达式（ ）可以捕获所有发往或来自IP地址192.168.1.100的HTTPS流量。	http.host == 192.168.1.100	ip.addr == 192.168.1.100 && tcp.port == 443	http.request.method == "GET" && ip.addr == 192.168.1.100	ip.addr == 192.168.1.100 && tcp.port == 80
4157	单项选择题	密评过程中对网络信道中的IPSec协议数据包进行分析时，发现IKE Attribute显示加密算法ID为129，那么该协议使用的加密算法是（ ）。	SM1	SM4	SM7	AES
4158	单项选择题	GB/T 33190《电子文件存储与交换格式 版式文档》中定义的（ ）格式是我国发布的一种自主格式，在电子证照、电子发票、电子签章等领域广泛应用。	PDF	CFD	OFD	KFD
4159	单项选择题	密评过程中使用Wireshark工具对网络信道中的SSL协议数据进行分析时，可以在（ ）数据报文中获取通信双方所协商的密码套件。	Client Hello	Server Hello	Server Key Exchange	Client Key Exchange
4160	单项选择题	密评过程中使用Wireshark工具对网络信道中的SSL协议数据进行分析时，可以在（ ）数据报文中获取客户端所支持的密码套件。	Client Hello	Server Hello	Server Key Exchange	Client Key Exchange
4161	单项选择题	密评过程中对网络信道中的IPSec协议数据进行分析时，IKE Attribute显示杂凑算法ID为20，那么该协议所使用的杂凑算法是（ ）。	SM3	SHA1	MD5	SHA-256

4162	单项选择题	密评过程中对网络信道中的IPSec协议数据进行分析时，IKE Attribute显示算法ID为2，那么该协议所使用的公钥算法算法是（ ）。	RSA-1024	SM2	SM9	RSA-2048
4163	单项选择题	密评过程中对网络信道中的SSL协议数据进行分析时，可以在（ ）数据报文中获取客户端发给服务端的随机数。	Client Hello	Server Hello	Server Key Exchange	Client Key Exchange
4164	单项选择题	密评过程中对网络信道中的SSL协议数据进行分析时，可以在（ ）数据报文中获取服务端发给客户端的随机数。	Client Hello	Server Hello	Server Key Exchange	Client Key Exchange
4165	单项选择题	若一个数字证书的keyUsage扩展项包含nonRepudiation，表明该证书为（ ）。	加密证书	签名证书	CA证书	终端实体证书
4166	单项选择题	密评过程中对网络信道中的IPSec协议数据进行分析时，在协议的（ ）阶段可以获得通信双方所协商采用的密码算法。	ISAKMP协议主模式	ISAKMP协议快速模式	AH协议	ESP协议
4167	单项选择题	Linux系统的用户口令一般存储在/etc/shadow路径下，口令存储字符串格式为：idsalt$encrypted，其中id为2时表示口令采用（ ）密码算法进行杂凑后存储。	MD5	Blowfish	SHA-256	SHA-512
4168	单项选择题	Linux系统的用户口令一般存储在/etc/shadow路径下，口令存储字符串格式为：idsalt$encrypted，其中id为5时表示口令采用（ ）密码算法进行杂凑后存储。	MD5	Blowfish	SHA-256	SHA-512
4169	单项选择题	Linux系统的用户口令一般存储在/etc/shadow路径下，口令存储字符串格式为：idsalt$encrypted，其中id为6时表示口令采用（ ）密码算法进行杂凑后存储。	MD5	Blowfish	SHA-256	SHA-512

4170	单项选择题	对数字证书进行解析时，发现证书的签名算法OID是1.2.156.10197.1.501，那么该证书使用的密码算法是（ ）。	基于SM2算法和SM3算法的签名	基于RSA算法和SM3算法的签名	基于SM9算法和SHA-256算法的签名	基于SM2算法和SHA-256算法的签名
4171	单项选择题	在测评过程中会常遇到的以"-----BEGIN..."开头，"-----END..."结尾的数据编码格式是（ ）。	Base64	PEM	BER	DER
4172	单项选择题	密评过程中，采用端口扫描主要用于探测和识别被测信息系统中的VPN、服务器密码机、数据库服务器等设备开放的端口服务。IPSec VPN中IKE协议常用的UDP端口号是（ ）。	500	450	4500	5000
4173	单项选择题	密评过程中，采用端口扫描主要用于探测和识别被测信息系统中的VPN、服务器密码机、数据库服务器等设备开放的端口服务。IPSec VPN中通常为了穿透NAT设备会开放UDP端口号（ ）。	500	450	4500	5000
4174	单项选择题	密评过程中，依据（ ）标准对数据的随机性进行分析。	GM/T 0105《软件随机数发生器总体框架》	GM/T 0028《密码模块安全技术要求》	GM/T 0005《随机性检测规范》	GM/T 0039《密码模块安全检测要求》
4175	单项选择题	密评过程中，依据（ ）标准对数字证书格式的合规性进行分析。	GM/T 0015《基于SM2密码算法的数字证书格式规范》	GM/T 0028《密码模块安全技术要求》	GM/T 0005《随机性检测规范》	GM/T 0034《基于SM2密码算法的证书认证系统密码及其相关安全技术规范》
4176	单项选择题	对数字证书格式进行分析时，无法获得的信息是（ ）。	CA对该证书的签名算法	该证书的有效日期	该证书的用途	该证书是否被撤销等有效状态
4177	单项选择题	在密评中，以下（ ）设备一般不作为测评工具接入点。	防火墙	交换机	服务器	堡垒机
4178	单项选择题	一般无法通过分析SSL协议数据获得的是（ ）。	通信协议使用的密码套件	握手协议过程	ISAKMP的协议过程	记录协议过程

4179	单项选择题	通过对网络信道中的IPSec协议数据进行分析时，无法获得的信息是（ ）。	使用的加密算法	使用的完整性保护算法	使用的鉴别机制	会话密钥明文
4180	单项选择题	通过对网络信道中的SSL协议数据进行分析时，Server Hello中显示密码套件ID为{0xe0,0x11}，则表示双方所协商的密钥交换算法和加密算法分别为（ ）。	SM2密钥交换算法，SM4_CBC	RSA公钥加密算法，AES_CBC	RSA公钥加密算法，SM4_CBC	SM2密钥交换算法，SM1_CBC
4181	单项选择题	通过对网络信道中的SSL协议数据进行分析时，Server Hello中显示密码套件ID为{0xe0,0x13}，则表示双方所协商的密钥交换算法和加密算法分别为（ ）	SM2密钥交换算法，SM1_CBC	SM2公钥加密算法，SM4_CBC	SM2密钥交换算法，SM4_CBC	SM2公钥加密算法，SM1_CBC
4182	单项选择题	通过对网络信道中的国密SSL协议数据进行分析时，按照GM/T 0024《SSL VPN技术规范》，实现标识为ECC的密码算法和实现标识为IBC的算法分别为（ ）	SM3，SM2	ECDSA，RSA	SM2，SM9	SM3,SM9
4183	单项选择题	SSL协议密钥协商过程中，如果密钥交换算法为ECC，则客户端应产生预主密钥，并采用服务端的（ ）进行加密并放在Client Key Exchange消息中发送给服务端。	签名私钥	签名私钥	签名公钥	加密公钥
4184	单项选择题	SSL协议密钥协商过程中，如果密钥交换算法为ECDHE，则Client Key Exchange消息包含计算（ ）的客户端密钥交换参数。	工作密钥	根密钥	主密钥	预主密钥
4185	单项选择题	通过对网络信道中的SSL协议数据进行分析，Server Hello中显示密码套件ID为{0xe0,0x53}，则表示双方所协商的密钥交换算法为和加密算法分别为（ ）	SM2公钥加密算法，SM4_CBC	SM2密钥交换算法，SM4_CBC	SM2密钥交换算法，SM4_GCM	SM2公钥加密算法，SM4_GCM
4186	单项选择题	通过对网络信道中的SSL协议数据进行分析，Server Hello中显示密码套件ID为{0xe0,0x17}，则表示双方所协商的密钥交换算法为和加密算法分别为（ ）	SM2公钥加密算法，SM4_CBC	SM9公钥加密算法，SM4_CBC	SM9公钥加密算法，SM4_GCM	SM2公钥加密算法，SM4_GCM

4187	多项选择题	密评过程中,以下属于测评实施方式的是（ ）。	随机性检测	数字证书格式合规性检测	IPSec/SSL协议分析	端口扫描
4188	多项选择题	通过对数字证书格式进行分析，无法获得的信息是（ ）。	证书格式是否合规	证书签名结果是否正确	证书由谁签发	证书用于哪个协议的密钥交换或者身份鉴别
4189	多项选择题	密评过程中，以下能获取的数据是（ ）。	SSL协议通信数据	IPSec协议通信数据	远程管理通道数据	密码机内的密钥数据明文
4190	多项选择题	以下能进行密码算法正确性验证的是（ ）。	密码杂凑算法	数字签名算法	分组密码算法	虹膜识别算法
4191	多项选择题	在密评中，以下属于测评实施内容的是（ ）。	密码算法实现正确性检测	数字证书格式合规性检测	随机数质量检测	与密码相关的漏洞识别
4192	多项选择题	使用Wireshark进行网络数据报文抓取后的数据一般以（ ）格式存储。	.pcap	.pcapng	.cap	.cer
4193	多项选择题	以下哪些工具可用于密评工作（ ）。	Wireshark	端口扫描工具	渗透测试工具	逆向分析工具
4194	多项选择题	对数字证书分析时，其数字证书的扩展名是cer，那么它可能的编码方式是（ ）。	BASE64编码	二进制DER编码	Goppa编码	BCH编码
4195	多项选择题	某证书的签名算法是1.2.156.10197.1.501，则意味着（ ）。	该证书所包含的公钥是SM2公钥	签发该证书采用的是SM3withSM2Encryption算法	颁发者所使用的公钥是SM2公钥	不考虑编码，该证书的签名值长度应为64字节
4196	多项选择题	对数字证书进行解析时，发现该证书的公钥对应的类型是1.2.156.10197.1.301，则意味着（ ）。	该证书所包含的公钥是SM2公钥	签发该证书采用的是SM3withSM2Encryption算法	颁发者所使用的公钥是SM2公钥	不考虑编码，该证书所包括的公钥长度应为64字节
4197	多项选择题	某信息系统使用签名验签服务器对合同进行数字签名后，通过受SSL协议保护的信道发送给用户，在测评时，可以通过（ ）采集合同及数字签名值进行测评。	获取应用程序调用签名验签服务器的报文	从受SSL协议保护信道中获取发送给用户的数据	在用户端获取合同以及数字签名值	在应用程序所在的服务器获取合同以及数字签名值

4198	多项选择题	用户通过安全浏览器与SSL VPN搭建的SSL通道，与信息系统所属内网的应用服务器进行数据通信，那么从以下（）位置可以抓取到SSL报文。	用户使用安全浏览器的终端	SSL VPN内部	安全浏览器与SSL VPN之间的通信信道	信息系统所属内网的服务器
4199	多项选择题	在验证某个密文是否由SM2算法加密时，如果可以知道明文和公钥，但无法获得私钥时，以下方法中可行，并且可以作为证据的是（）。	分析该密文开头的64字节是否是SM2椭圆曲线上的点	对明文进行公钥加密，对比产生密文是否与待测密文一致	分析明密文长度是否相差96字节	分析密文长度是否是512字节
4200	多项选择题	以下（）方法可以用于辅助数字证书的分析。	对数字证书的数字签名算法进行正确性验证	对数字证书进行随机性检测	使用ASN.1工具对数字证书格式进行解析	对数字证书的杂凑密码算法进行正确性验证
4201	多项选择题	某信息系统中部署了IPSec VPN对网络信道进行保护，通过分析信道中的IPSec协议数据，可以获取的信息是（）。	ISAKMP主模式中的签名证书	ISAKMP主模式中的加密证书	ISAKMP快速模式中的载荷（除ISAKMP头外）	ISAKMP主模式中响应方生成的临时密钥
4202	多项选择题	一般对数据进行随机性检测的内容包括（）。	单比特频数检测	块内频数检测	块间频数检测	扑克检测
4203	多项选择题	以下可用于协议数据采集的工具有（）。	Wireshark	tcpdump	BusHound	Fiddler
4204	多项选择题	AES密码算法支持哪些密钥长度（）。	128比特	192比特	512比特	256比特
4205	多项选择题	证书撤销列表CRL的数据结构中包括（）。	tbsCertList	tbsCertificate	signatureAlgorithm	signatureValue
4206	多项选择题	对数字证书格式进行分析时，可以分析数字证书的各个字段，一个数字证书的数据结构包括（）。	tbsCertList	tbsCertificate	signatureAlgorithm	signatureValue
4207	多项选择题	在测评时发现某信息系统数据库中某数据杂凑值长度为256比特，则其使用的算法可能为（）。	SHA3-256	SM3	SHA-256	SHA1
4208	多项选择题	在测评时发现某信息系统数据库中某数据密文长度为160字节，则其使用的算法可能为（）。	SM4	AES-128	AES-192	DES
4209	多项选择题	Base64是基于64个可打印的字符来表示二进制数据的一种方法，以下属于64个可打印字符的是（）。	A到Z	0至9	a到z	$

4210	多项选择题	一般数字证书的后缀名是（ ）。	cer	crt	der	pem
4211	多项选择题	数字证书格式中，keyUsage扩展项可以判断证书的用途，当设置了（ ）位中的一位时，表示该证书为签名证书。	digitalSignature	nonRepudiation	keyAgreement	keyEncipherment
4212	多项选择题	对数字证书分析，一般要分析哪些内容（ ）。	查看数字证书格式	查看数字证书密钥用法	验证数字证书数字签名	验证数字证书链
4213	多项选择题	通过对网络信道中的SSL协议数据包进行分析，能够看到以下哪些信息（ ）。	查看Hello消息的密码套件	查看派生出的主密钥	解密ESP封装的报文	查看服务端证书
4214	多项选择题	根据GM/T 0005《随机性检测规范》，可以对被测数据的（ ）进行分析。	单比特频数检测	自相关性	完整性	不可否认性
4215	多项选择题	CA对RSA公钥数字证书进行签名的算法可能是（ ）	RSA-2048	HMAC-SHA256	SM2	ECDSA
4216	多项选择题	通过对网络信道中的IPSec协议数据包进行分析，密评人员可以获得以下哪些信息（ ）。	IPSec协议建立过程中双方协商的密码算法	IPSec协议建立过程中双方的证书	IPSec协议建立过程中双方协商的会话密钥	IPSec协议的报文封装协议
4217	多项选择题	在密评中，使用Wireshark对网络通道的SSL协议数据进行抓取，描述不正确的有（ ）。	可接入到安装有国密SSL安全浏览器的客户端，捕获SSL协议建立过程的数据包	一定可以查看到握手协议中双方的身份证书	可查看到双方协商的用于密钥协商的算法	可以在不需要双方公私钥对的情况下，解密SSL协议记录层保护的数据
4218	多项选择题	密码算法合规性检测，包括对（ ）的检测。	SM3	虹膜识别算法	ZUC	SM9
4219	多项选择题	通过数字证书格式的分析，可以对数字证书解析出以下信息（ ）。	CA的签名算法	证书有效期	该证书公钥值	密钥用法
4220	多项选择题	下列（ ）选项是Base64编码的优点。	可以将二进制数据转换为可打印字符，方便传输	编码后的数据比原始数据更小，减少传输流量	可以用于加密数据，保护数据安全	可以避免传输中特殊字符被截断或转义的问题
4221	多项选择题	某数据库中存储的口令杂凑字段，长度为256比特，而且所有数据中存在少许相同的杂凑值，以下推断正确的是（ ）。	可能采用了SHA-1算法进行口令杂凑	可能采用了SM3算法进行口令杂凑	口令杂凑的过程中，可能使用了每个用户不同的盐值	口令杂凑的过程中，可能未加入盐值

4222	多项选择题	以下关于Wireshark过滤规则的说法，（ ）是正确的。	icmp and ip.dst==192.168.1.1 可以用于获取目标IP地址为192.168.1.1并且协议为ICMP的所有数据包	dns.dstport==53 and ip.src==192.168.1.1 用于获取所有源IP地址为192.168.1.1并且目标端口号为53的所有DNS请求数据包	udp.dstport==00:11:22:33:44:55 可以用于获取目标MAC地址为00:11:22:33:44:55并且协议为UDP的所有数据包	eth.dst==00:11:22:33:44:55可以用于获取所有目标MAC地址为00:11:22:33:44:55的数据包
4223	多项选择题	某信息系统在网络边界处部署了SSL VPN网关，为互联网终端访问内网资源建立安全传输通道，测评人员在以下接入点（ ）无法捕获SSL协议通信数据包。	SSL VPN网关上	SSL VPN网关与互联网终端之间的交换机上	信息系统内的应用服务器上	SSL VPN网关与信息系统应用服务器之间的核心交换机上
4224	多项选择题	测评人员通过数字证书格式进行，可以分析数字证书的以下信息（ ）。	版本号	序列号	签名算法	主体信息
4225	多项选择题	某信息系统用户口令使用加盐后再计算杂凑值的方式进行存储保护，杂凑算法为SHA-256，测评人员如果想验证杂凑值计算的正确性，需要知道以下信息（ ）。	盐值	口令明文	杂凑值	盐值与口令的组合方式
4226	多项选择题	某机构A与分支机构B之间通过成对部署IPSec VPN网关建立安全传输通道，测评人员想要捕获两个IPSec VPN之间的通信数据包，可在以下位置（ ）接入数据采集工具。	机构A部署的IPSec VPN	分支机构B部署的IPSEC VPN	机构A的用户PC端	机构B的用户PC端
4227	多项选择题	某信息系统管理员通过远程管理终端访问SSL VPN，再通过VPN访问堡垒机，最后通过堡垒机对通用服务器进行远程管理。以下哪个接入点能够捕获远程管理终端与SSL VPN网关之间的通信数据（ ）。	远程管理终端	SSL VPN	堡垒机	通用服务器
4228	多项选择题	以下可能通过Wireshark解析出的密码套件有（ ）。	ECDHE_SM4_CBC_SM3	ECDHE_SM4_GCM_SM3	IBC_SM4_CBC_SM3	ECC_SM4_CBC_SM3

4229	多项选择题	对于Wireshark的使用，以下方式合理的有（ ）。	使用tcpdump采集通信数据后，再用Wireshark分析通信数据包的密码应用情况	在用户PC端所连接的交换机通过端口镜像的方式采集数据，再离线使用Wireshark对通信数据包的密码应用情况进行分析	在用户PC端使用Wireshark对PC端与SSL VPN之间的通信数据进行采集和分析	将Wireshark安装到应用服务器上，对互联网用户通过SSL VPN访问内网资源的网络层通信数据进行采集分析
4230	多项选择题	ASN.1中支持哪些基本类型（ ）。	INTEGER	BOOLEAN	OCTET STRING	SET
4231	多项选择题	一个数据的ASN.1编码如下：{0x02,0x12，……}，那么以下说法正确的是（ ）。	这是一个整数（INTEGER）	这是一个序列（SEQUENCE）	其实际数据长度是12字节	其实际数据长度是18字节
4232	多项选择题	一个数据的ASN.1编码如下：{0x30,0x12，……}，那么以下说法正确的是（ ）。	这个类型是一个无序的结构	这是一个序列（SEQUENCE）	其实际数据长度是18字节	其实际数据长度是12字节
4233	多项选择题	一个数据的ASN.1编码如下：{0x30,0x81,OxFF,……}，那么以下说法正确的是（ ）。	这是一个序列（SEQUENCE）	其实际数据长度是81字节	其实际数据长度是255字节	其实际数据长度是129字节
4234	多项选择题	一个数据的ASN.1编码如下：{0x30,0x82,Ox01,0x00,……}，那么以下说法正确的是（ ）。	这是一个序列（SEQUENCE）	其实际数据长度是82字节	其实际数据长度是100字节	其实际数据长度是256字节
4235	多项选择题	以下关于Wireshark过滤规则的说法，（ ）是正确的。	tcp.port==80可以用于获取所有目标端口为80的TCP数据包	ip.src==192.168.1.1 and ip.dst==192.168.1.2可以用于获取源IP地址为192.168.1.1，目标IP地址为192.168.1.2的所有数据包	ip.addr==192.168.1.1 and not tcp.port==22可以用于获取目标IP地址为192.168.1.1且不是SSH协议的所有数据包	ip.addr==192.168.1.1 and ip.addr==192.168.1.2可以用于获取源IP地址为192.168.1.1且目标IP地址为192.168.1.2的所有数据包

4236	多项选择题	以下关于Wireshark过滤规则的说法，（ ）是正确的。	tcp.port==443可以用于获取所有目标端口为443的TCP数据包	ip.addr==192.168.1.1可以用于获取源或目标IP地址为192.168.1.1的所有数据包	arp.src.hw_mac==00:11:22:33:44:55可以用于获取源MAC地址为00:11:22:33:44:55的ARP数据包	http.response.code==200可以用于获取所有HTTP响应状态码为200的数据包
4237	判断题	当测评工具接入信息系统条件不成熟时，应与被测单位协商，生成必要的离线数据。	正确	错误		
4238	判断题	如果证书相关的算法标识符合要求，则认为该证书是合规的。	正确	错误		
4239	判断题	IPSec协议分析时主要是分析IPSec协议使用的密码算法信息，不需要对证书进行分析。	正确	错误		
4240	判断题	在密评实施过程中，由于无法获取密钥，因此除了密码杂凑算法的测试外，其他算法的正确性测试均无法开展。	正确	错误		
4241	判断题	对SM2签名结果的正确性进行测试时，如果可以获取SM2私钥，那么可以根据GB/T32918.2《信息安全技术 SM2椭圆曲线公钥密码算法 第二部分：数字签名算法》，重新进行SM2签名生成，比对生成的SM2签名是否与被测试的SM2签名值一致，如果不一致，则说明使用的不是SM2算法。	正确	错误		
4242	判断题	对SM2加密进行测试时，可以根据GB/T32918.4《信息安全技术 SM2椭圆曲线公钥密码算法 第四部分：公钥加密算法》，进行SM2密文的生成，比对生成的SM2密文是否与被测试的SM2密文一致，如果不一致，则说明使用的不是SM2加密算法。	正确	错误		

4243	判断题	在对数字证书进行分析时，发现用户的加密证书和签名证书虽然证书内容不同，但Key Usage均相同，这是一种正常情况。	正确	错误		
4244	判断题	如果IPSec VPN使用的是预共享密钥（PSK）方式，那么在采用Wireshark进行分析时抓取不到证书是正常的，也可以满足GM/T 0022 《IPSec VPN技术规范》的相关要求。	正确	错误		
4245	判断题	测评工具均基于确定的密码算法、协议等实现，因而不需要校准。	正确	错误		
4246	判断题	协议分析和端口扫描是等级保护测评时常用的测评实施方式，在密码应用安全性评估过程中不涉及上述实施方式。	正确	错误		
4247	判断题	对同一数据分别使用SHA-224和SHA3-224算法计算杂凑值，其输出长度是不一样的。	正确	错误		
4248	判断题	对同一数据分别使用SHA-256和SHA3-256算法计算杂凑值，其输出长度是不一样的。	正确	错误		
4249	判断题	对同一数据分别使用SHA-224和SHA-512/224算法计算杂凑值，其输出长度是一样的。	正确	错误		
4250	判断题	对同一数据分别使用SHA-256和SHA-512/256算法计算杂凑值，其输出长度是一样的。	正确	错误		
4251	判断题	对同一数据分别使用MD5和SHA1算法计算杂凑值，其输出长度是一样的。	正确	错误		
4252	判断题	ISAKMP快速模式中的载荷（除ISAKMP 头外）可以通过Wireshark进行解析。	正确	错误		
4253	判断题	通过Wireshark可以解析ESP协议中的数据字段。	正确	错误		

4254	判断题	通过Wireshark可以解析SSL协议中记录层的字段。	正确	错误		
4255	判断题	CA机构 可以为同一个实体以相同的甄别名称（Distinguished Name,DN）签发多张数字证书。	正确	错误		
4256	判断题	解析数字证书中的keyUsage扩展项，如果keyCertSign位被置为1，则表示该证书为CA证书。	正确	错误		
4257	判断题	用Windows系统自带解析工具查看数字证书，其中解析出的“指纹”字段即表示CA对该证书数字签名的结果。	正确	错误		
4258	判断题	GB/T 20518《信息安全技术 公钥基础设施 数字证书格式》规定CRL数据结构若包含version字段，必须是v2。	正确	错误		
4259	判断题	证书撤销列表CRL数据结构中的nextUpdate字段表明下一次CRL发布的时间不能早于该时间。	正确	错误		
4260	判断题	证书撤销列表CRL中列出了被撤销的数字证书的完整内容。	正确	错误		
4261	判断题	一个签名证书的keyUsage扩展项中的digitalSignature和nonRepudiation中的1位须置为1。	正确	错误		
4262	判断题	使用Wireshark获取的SSL协议数据，Server Hello中显示密码套件ID为{0xe0,0x13}，则表示双方所协商的密钥交换算法为SM2公钥加密，加密算法为SM4。	正确	错误		
4263	判断题	使用Wireshark获取的SSL协议数据，Server Hello中显示密码套件ID为{0xe0,0x11}，则表示双方所协商的密钥交换算法为SM2密钥交换，加密算法为SM4。	正确	错误		
4264	判断题	在IPSec VPN中，如果采用隧道模式，则ESP协议的加密范围和认证范围是一致的。	正确	错误		

4265	判断题	在IPSec VPN中，如果采用传输模式，则ESP协议的加密范围和认证范围是不一致的。	正确	错误		
4266	判断题	Wireshark是对网络和通信安全层面进行测评常用的工具。	正确	错误		
4267	判断题	随机性检测应包括GM/T 0005《随机性检测规范》中的单比特频数检测、扑克检测等12项检测。	正确	错误		
4268	判断题	如果一张数字证书的公钥字段是RSA2048，那么签发这张证书的签名算法不可能是SM3withSM2。	正确	错误		
4269	判断题	Wireshark可以帮助密评人员核实在IPSec协议Hello消息中，通信双方协商的密码算法。	正确	错误		
4270	判断题	密评人员可通过Wireshark，确认SSL协议握手阶段采用的是单向鉴别还是双向鉴别机制。	正确	错误		
4271	判断题	分析数字证书格式时，通过ASN.1 DER格式展示证书签名值（采用SM2签名算法），该字段TLV三元组长度为64字节。	正确	错误		
4272	判断题	在做SM2签名验证时，提供以下数据：消息/摘要值、公钥值、签名值、随机数。	正确	错误		
4273	判断题	密评人员在对密码算法进行分析时，若遇到SM4-CBC加密模式，应进一步确认算法的填充方式。	正确	错误		
4274	判断题	测评人员在对某三级信息系统进行密评时，发现测评工具接入被测信息系统条件还不成熟，因此测评人员只能等到条件成熟时才能继续开展测评。	正确	错误		
4275	判断题	在使用Wireshark进行信息系统密码应用测评时，Wireshark只能从被测信息系统边界设备上接入并进行数据采集。	正确	错误		

4276	判断题	在对信息系统进行密评时，测评人员需要获取存储在密码机内部的密钥，并分析该密钥的随机性进而确定密钥生成是否符合要求，以此作为“密钥管理安全性”判定结果的考虑依据。	正确	错误		
4277	判断题	移动终端用户通过互联网经SSL VPN访问内网资源，测评人员可以在移动终端上接入Wireshark，对移动终端用户与SSL VPN网关之间通信信道密码应用的合规、正确和有效性进行分析。	正确	错误		
4278	判断题	密评时对SSL协议进行抓包分析以验证密码算法合规性，主要抓取的是记录层协议的数据包。	正确	错误		
4279	单项选择题	若某信息系统中“应急处置”层面所有测评指标都不适用，而其他各层面均为适用的测评指标，根据《商用密码应用安全性评估量化评估规则（2021版）》进行量化评估时，分值计算公式的分母为（ ）。	90	92	94	100
4280	单项选择题	根据《商用密码应用安全性评估量化评估规则（2021版）》，若信息系统使用认证合格的密码产品基于SM4-CBC算法实现了重要数据存储机密性保护，但该密码产品的密码模块安全等级低于应达到的安全等级要求，则其“重要数据存储机密性”测评单元的量化评估结果为（ ）。	1	0.5	0.25	无法判断
4281	单项选择题	根据《商用密码应用安全性评估量化评估规则（2021版）》，某信息系统使用签名验证服务器（获得商用密码产品认证证书）实现SM2数字签名功能，在设备和计算层面对签名验签服务器进行量化评估时，其结果为（ ）。	1	0.5	0	无法判断

4282	单项选择题	根据《商用密码应用安全性评估量化评估规则（2021版）》，对某四级信息系统进行量化评时，物理和环境安全层面身份鉴别、电子门禁记录数据存储完整性、视频记录数据存储完整性三个测评单元得分分别为0.5分、0.5分、0.5分，则该层面量化评估的最终得分为（ ）。	0.6296	0.6667	0.8333	0.5
4283	单项选择题	根据《商用密码应用安全性评估量化评估规则（2021版）》，对某三级信息系统进行量化评估时，物理和环境安全层面身份鉴别、电子门禁记录数据存储完整性、视频记录数据存储完整性三个测评单元得分分别为不适用、0.5分、1分，则该层面量化评估的得分为（ ）。	0.75	0.6667	0.4375	0.5
4284	单项选择题	根据《商用密码应用安全性评估量化评估规则（2021版）》，对某三级信息系统进行量化评估时，共选取了四条通信信道作为网络和通信安全层面测评对象，在身份鉴别测评单元中，四条通信信道的测评结果分别为1分、0.25分、0.5分、不适用，则身份鉴别测评单元的量化评估结果为（ ）。	0.25	0.4375	0.5833	0.6667
4285	单项选择题	对某三级信息系统进行量化评估时，设备和计算层面某一个测评对象涉及2台设备，这2台设备在日志记录完整性测评单元测评结果得分分别为0.5分、0.25分。根据《商用密码应用安全性评估量化评估规则（2021版）》，该测评对象在日志记录完整性测评单元的量化评估结果为（ ）。	0.25	0.375	0.5	无法判断

4286	单项选择题	某信息系统调用经检测认证合格的签名验签服务器，使用SM3算法对数据库存储的重要数据进行完整性保护，该签名验签服务器符合相应的密码模块安全等级要求。根据《商用密码应用安全性评估量化评估规则（2021版）》，“重要数据存储完整性”测评单元的量化评估结果为（ ）。	0	0.25	0.5	1
4287	单项选择题	某信息系统基于OpenSSL软件实现的RSA-2048算法，对用户登录口令的传输机密性进行保护。根据《商用密码应用安全性评估量化评估规则（2021版）》，该信息系统在应用和数据安全层面的身份鉴别的量化评估结果为（ ）。	0	0.25	0.5	1
4288	单项选择题	根据《商用密码应用安全性评估量化评估规则（2021版）》，某三级信息系统采用经检测认证合格的服务器密码机（密码模块安全等级为一级），通过SM4算法对用户登录口令的传输进行机密性保护，其应用和数据安全层面的数据传输机密性指标的量化评估结果为（ ）。	0	0.25	0.5	1
4289	单项选择题	根据《商用密码应用安全性评估量化评估规则（2021版）》，某信息系统测评时，网络和通信安全层面整体不适用，但其他安全层面得分均为满分，则对该信息系统量化评估时，结果为（ ）。	80	85	90	100
4290	单项选择题	根据《商用密码应用安全性评估量化评估规则（2021版）》，某三级信息系统密评时所有安全层面均适用，建设运行层面五个测评单元得分分别为1分、0.5分、0.5分、1分、0分，则该层面量化评估的得分为（ ）。	0.3064	0.6477	0.8001	0.9112

4291	单项选择题	根据《商用密码应用安全性评估量化评估规则（2021版）》，某三级信息系统密评时所有安全层面均适用，建设运行层面五个测评单元得分分别为1分、0.5分、0.5分、1分、不适用，单元指标权重分别是1，1，0.7，1，0.7，则该层面量化评估的得分为（ ）。	0.3064	0.5011	0.7703	0.9112
4292	单项选择题	根据《商用密码应用安全性评估量化评估规则（2021版）》，某三级信息系统中，用户登录过程中使用智能密码钥匙（经检测认证的二级密码模块）进行签名，服务器使用服务器密码机（经检测认证的一级密码模块）进行签名验证，同时智能密码钥匙使用获得电子认证服务密码使用许可证的CA机构签发的SM2数字证书，该登录用户的身份鉴别过程量化评估结果较为合理的是（ ）。	0	0.25	0.5	1
4293	单项选择题	根据《商用密码应用安全性评估量化评估规则（2021版）》，某三级信息系统密评时所有安全层面均适用，经测评，“物理和环境安全”、“网络和通信安全”、“设备和计算安全”、“应用和数据安全”量化评估结果分别为0.5、0.75、0.3333，0.6667，该系统上述4个层面整体量化评估结果为（ ）。	41.25	43.33	58.93	61.9
4294	单项选择题	根据《商用密码应用安全性评估量化评估规则（2021版）》，从DAK三个角度对信息系统进行量化评估，其中D表示（ ）。	密码算法合规性	密码算法有效性	密码使用合规性	密码使用有效性

4295	单项选择题	某三级测绘系统用户基于SM2数字证书登录系统，SM2数字证书存储在智能密码钥匙（经检测认证的二级密码模块）中，数字证书由具有电子认证服务密码使用许可证的第三方CA机构签发，并且用户与服务器之间的身份鉴别过程符合相关标准规范要求。根据《商用密码应用安全性评估量化评估规则（2021版）》，该用户的身份鉴别量化评估结果为（ ）。	0	0.25	0.5	1
4296	单项选择题	根据《商用密码应用安全性评估量化评估规则（2021版）》，若三级信息系统使用密码产品（经检测认证合格）中的AES-256算法实现身份鉴别数据的存储机密性保护，同时使用该密码产品中的SM4算法实现重要业务数据的存储机密性保护，则身份鉴别数据存储机密性和重要业务数据存储机密性的分值分别最多为（ ）。	0，0	0.25，0.5	0.5，1	0.5，0.5
4297	单项选择题	某三级电力系统通过部署安全认证网关（经检测认证的二级密码模块）实现通信数据安全传输。经抓包分析，该通信信道上采用了电力专用的SSF09算法实现通信数据的机密性保护，经咨询行业主管部门和密码主管部门，SSF09算法属于密码主管部门批准使用的算法，则根据《商用密码应用安全性评估量化评估规则（2021版）》，该通信信道上数据传输机密性保护的量化评估结果为（ ）。	0	0.25	0.5	1

4298	单项选择题	根据《商用密码应用安全性评估量化评估规则（2021版）》，信息系统在对应用和数据安全层面测评过程中发现重要业务数据使用SM3算法实现数据存储的完整性保护，则该测评对象的“数据存储完整性保护”的量化评估结果为（ ）。	0	0.25	0.5	1
4299	单项选择题	根据《商用密码应用安全性评估量化评估规则（2021版）》，某三级信息系统在对网络和通信安全层面测评过程中发现，非国密浏览器（未通过商用密码检测认证）和安全认证网关（经检测认证的二级密码模块）之间通信信道使用自签的RSA-2048数字证书进行身份鉴别，则该测评对象在“身份鉴别”的量化评估结果为（ ）。	0	0.25	0.5	1
4300	单项选择题	根据《商用密码应用安全性评估量化评估规则（2021版）》，某二级信息系统对应用和数据安全层面测评过程中发现，系统通过调用服务器密码机（经检测认证的一级密码模块）使用AES-256算法实现个人敏感信息存储的机密性保护，则该测评对象的量化评估结果为（ ）。	0	0.25	0.5	1
4301	单项选择题	根据《商用密码应用安全性评估量化评估规则（2021版）》，在对某三级信息系统进行“建立上岗人员培训制度”测评单元测评时，若仅制定了相关人员培训制度，但未提供《培训内容纪要》和《培训人员签到表》，则该测评单元的量化评估结果为（ ）。	0	0.25	0.5	1

4302	单项选择题	根据《商用密码应用安全性评估量化评估规则（2021版）》，某三级网银系统用户通过智能密码钥匙（经检测认证的二级密码模块）使用美国GlobalSign颁发的SHA-256WtihRSA-2048算法数字证书登录网银系统，则该测评对象分值最合理的是为（）。	0	0.25	0.5	1
4303	单项选择题	根据《商用密码应用安全性评估量化评估规则（2021版）》，以下哪个方面不属于量化评估需要考虑的方面（）。	密码使用有效性	密码算法/技术合规性	密钥管理安全	密码算法/技术实现正确性
4304	单项选择题	根据《商用密码应用安全性评估量化评估规则（2021版）》，在量化评估框架中，字母D表示（）。	Cryptography Deployment Effectiveness	Cryptography Data Security	Key Distribution Security	Cryptography Deployment Security
4305	单项选择题	根据《商用密码应用安全性评估量化评估规则（2021版）》，在量化评估框架中，字母K表示（）。	Cryptography Key Security	Key management security	Key confidentiality	Cryptographic key lifecycle management
4306	单项选择题	根据《商用密码应用安全性评估量化评估规则（2021版）》，在量化评估框架中，字母A表示（）。	Adherence to cryptographic algorithm standards	Cryptographic algorithm validation	Cryptography Algorithm compliance	Algorithmic review and approval
4307	单项选择题	根据《商用密码应用安全性评估量化评估规则（2021版）》，在密码应用技术各层面的测评对象的量化评估结果可能是（）。	{0,0.5,1}	{0,0.25,0.5,1}	{0,1}	{0,0.5,0.75,1}
4308	单项选择题	根据《商用密码应用安全性评估量化评估规则（2021版）》，在密码应用技术层面中，某个测评单元量化评估通常为该单元内所有测评对象结果的（）。	最大值	加权平均值	算术平均值	几何平均值
4309	单项选择题	根据《商用密码应用安全性评估量化评估规则（2021版）》，测评单元量化结果的小数处理采取的方法是（）。	向上取整	向下取整	直接舍弃	四舍五入

4310	单项选择题	根据《商用密码应用安全性评估量化评估规则（2021版）》，密码应用管理要求各安全层面的量化评估取值可能是（ ）。	{0,0.25,0.5,1}	{0,0.5,1}	{0,1}	[0,1]
4311	单项选择题	根据《商用密码应用安全性评估量化评估规则（2021版）》，某个安全层面的量化评值通常为该安全层面内所有测评单元结果的（ ）。	最大值	加权平均值	算术平均值	几何平均值
4312	单项选择题	根据《商用密码应用安全性评估量化评估规则（2021版）》，各安全层面的量化结果的小数处理采取的方法是（ ）。	向上取整	向下取整	直接舍弃	四舍五入
4313	单项选择题	根据《商用密码应用安全性评估量化评估规则（2021版）》，安全层面的测评结果需要保留小数点后（ ）位。	1	2	3	4
4314	单项选择题	根据《商用密码应用安全性评估量化评估规则（2021版）》，已知某个测评单元有5个测评对象，量化评估结果分别为1，1，1，1，0，则该测评单元得分为（ ）。	1	0	0.8	0.5
4315	单项选择题	在物理和物理和环境安全层面，某个信息系统所在机房，采用指纹技术对进入机房的用户进行身份鉴别，根据《商用密码应用安全性评估量化评估规则（2021版）》，该对象的量化评估结果为（ ）。	0	0.25	0.5	1
4316	单项选择题	在物理和环境安全层面，某个机房采用具有商用密码产品认证证书的门禁系统，满足GM/T 0036《采用非接触卡的门禁系统密码应用技术指南》的要求，并采用HMAC-SM3算法实现日志的完整性保护，根据《商用密码应用安全性评估量化评估规则（2021版）》，该“电子门禁记录数据完整性”的量化评估结果最合理的为（ ）。	无法判定	0.25	0.5	1

4317	单项选择题	在某个政务三级信息系统的网络和通信安全层面测评过程中，发现该系统采用获得电子认证服务密码使用许可证的CA机构签发的数字证书，该证书存放在智能钥匙（经检测认证的二级密码模块）中，证书的签名算法Oid标识为1.2.156.10197.1.501，证书在有效期内，身份鉴别过程采用SM2算法，根据《商用密码应用安全性评估量化评估规则（2021版）》，该层面的身份鉴别量化结果为（）。	0	0.25	0.5	1
4318	单项选择题	在某个政务三级信息系统的网络和通信安全层面测评过程中，发现采用了SSL VPN设备（经检测认证的二级密码模块）实现通信链路数据的安全传输。通过抓包分析，采用的密码套件为RSA_SM4_SM3，根据《商用密码应用安全性评估量化评估规则（2021版）》，该层面的“身份鉴别”的量化结果为（）。	0	0.25	0.5	1
4319	单项选择题	在某个政务三级信息系统的设备和计算层面测评过程中，发现采用了具有商用密码产品认证证书的SSL VPN设备，根据《商用密码应用安全性评估量化评估规则（2021版）》，该测评对象“日志记录完整性”的的量化结果为（）。	0	0.5	1	不确定

4320	单项选择题	某三级信息系统在设备和计算安全层面测评过程中，对某个密码设备（经检测认证的二级密码模块）进行测评时，发现设备的登录采用了WEB登录方式，登录界面需要输入用户名+口令，口令经过加盐使用SM3计算杂凑后传输，根据《商用密码应用安全性评估量化评估规则（2021版）》，该测评对象的“身份鉴别”的量化结果为（ ）。	0	0.5	1	不确定
4321	单项选择题	对于某三级系统，在设备和计算安全层面测评过程中，对某个密码设备（经检测认证的二级密码模块），发现设备的登录采用了WEB登录方式，登录界面需要输入用户名+口令，口令经过加盐并用SHA256计算杂凑后传输，根据《商用密码应用安全性评估量化评估规则（2021版）》，该测评对象的“身份鉴别”的量化结果为（ ）。	0	0.5	1	不确定
4322	单项选择题	在某个政务三级信息系统的设备和计算层面测评过程中，发现采用了具有商用密码产品认证证书的SSL VPN设备，根据《商用密码应用安全性评估量化评估规则（2021版）》，该测评对象“系统资源访问控制信息完整性”的量化结果为（ ）。	0	0.5	1	不确定
4323	单项选择题	在对某信息系统进行设备和计算层面测评过程中，某个测评单元具有3个测评对象，量化得分分别为1、1、0.5，根据《商用密码应用安全性评估量化评估规则（2021版）》，该测评单元的量化结果为（ ）。	0	0.5	0.8333	1

4324	单项选择题	在某信息系统进行设备和计算层面测评过程中，某个测评对象对应3个具体的设备，每个设备的D/A/K得分分别为1、0、0.5，根据《商用密码应用安全性评估量化评估规则（2021版）》，该测评对象的量化结果为（ ）。	0	0.25	0.5	1
4325	单项选择题	在三级信息系统测评中，在网络和通信层面，身份鉴别、通信数据完整性、通信过程中重要数据的机密性、网络边界访问控制信息的完整性、安全接入认证各测评单元得分为0、0.5、0.5、0、不适用，指标权重分别为，1、0.7、1、0.4、0.4，根据《商用密码应用安全性评估量化评估规则（2021版）》，该安全层面的量化得分为（ ）。	0.625	0.725	0.5	0.2741
4326	单项选择题	在三级信息系统测评中，在网络和通信层面，身份鉴别、通信数据完整性、通信过程中重要数据的机密性、网络边界访问控制信息的完整性、安全接入认证各测评单元得分为0、0.5、0.5、0、0，指标权重分别为1、0.7、1、0.4、0.4，根据《商用密码应用安全性评估量化评估规则（2021版）》，该安全层面的量化得分为（ ）。	0.6247	0.2429	0.5	0.725
4327	单项选择题	某三级信息系统于2019年10月建设完成并投入运行。2021年7月，该系统制定了密码应用改造方案并通过专家评审，2021年12月完成系统密码应用改造。根据《商用密码应用安全性评估量化评估规则（2021版）》，2022年1月，密评机构在对“制定密码应用方案”进行测评时，该测评单元的量化评估得分为（ ）。	0	0.5	1	不适用

4328	单项选择题	在三级系统测评中，某系被测信息系统为已在建运行系统，投入运行时间为2019年1月，该次测评为首次密评，则根据《商用密码应用安全性评估量化评估规则（2021版）》，建设运行层面“投入运行前进行密码应用安全性评估”测评项的量化得分为（ ）。	0	0.5	1	不适用
4329	单项选择题	某三级信息系统在测评过程中发现物理和环境安全层面不适用，网络和通信安全层面为0.625，设备和计算安全层面分值为0.4，应用和数据安全层面分值为0.5，安全管理四个层面分值均为1，根据《商用密码应用安全性评估量化评估规则（2021版）》，则该系统整体量化评估结果为（ ）。	61.5	68.3333	68.33	83.33
4330	多项选择题	根据《商用密码应用安全性评估量化评估规则（2021版）》，量化评估从（ ）方面进行。	密码使用正确性	密码使用有效性	密码算法/技术合规性	密钥管理安全
4331	多项选择题	根据《商用密码应用安全性评估量化评估规则（2021版）》，在密码应用技术层面中，某个测评单元量化评估结果可以是（ ）。	0.25	0.3333	0.5	1
4332	多项选择题	根据《商用密码应用安全性评估量化评估规则（2021版）》，以下关于量化评估过程，说法正确的是（ ）。	在判定密码使用有效性时，需综合考虑密码算法/技术合规性和密钥管理安全导致的风险	在判定密码使用有效性时，无需综合考虑密码算法/技术合规性和密钥管理安全导致的风险	若密码算法/技术合规性判定为不符合，则无需对密码使用有效性、密钥管理安全进行判定	若密码使用有效性判定为不符合，则无需对密码算法/技术合规性、密钥管理安全进行判定
4333	多项选择题	根据《商用密码应用安全性评估量化评估规则（2021版）》，以下密评量化评估结果中，应取小数点后4位的有（ ）。	测评对象	测评单元	安全层面	整体量化评估结果

4334	多项选择题	根据《商用密码应用安全性评估量化评估规则（2021版）》，以下说法正确的是（ ）。	若某测评指标不适用，则不参与量化评估过程	若某测评指标为特殊指标，则不参与量化评估过程	量化评估规则为每个测评单元分配了相应的权重，该权重与信息系统等级情况无关	量化评估规则为每个安全层面分配了相应的权重，该权重与信息系统等级情况无关
4335	多项选择题	根据《商用密码应用安全性评估量化评估规则（2021版）》，在测评对象量化评估中，以下得分为0.5的有（ ）。	D（√）A（√）K（√）	D（√）A（√）K（×）	D（√）A（×）K（√）	D（√）A（×）K（×）
4336	多项选择题	某三级信息系统，在内网接入区通过部署SSL VPN网关（经检测认证的二级密码模块）、国密浏览器（经检测认证的一级密码模块），实现对办公内网通道的密码应用改造。上述使用的密码产品均进行了正确的配置。根据《商用密码应用安全性评估量化评估规则（2021版）》，以下量化评估描述中，正确的有（ ）。	测评时使用国密览器访问系统时，发现其HTTPS协议使用的加密算法为SM4-GCM，该通道通信过程中重要数据的机密性测评单元量化评估结果为0.5	测评时使用国密浏览器访问系统时，发现其HTTPS协议使用的数字签名算法为RSA，该通道身份鉴别测评单元量化评估结果为0.5	测评时使用国密览器访问系统时，发现其HTTPS协议使用的MAC算法为HMAC-SM3，该通道通信过程中重要数据的机密性测评单元量化评估结果为1	测评时使用谷歌览器访问系统时，发现其HTTPS协议使用的MAC算法为HMAC-SHA1，该通道通信过程中重要数据的机密性测评单元量化评估结果为0.25
4337	多项选择题	对于双活机房间的物理裸光纤数据传输通道，根据《商用密码应用安全性评估量化评估规则（2021版）》，以下做法正确的包括（ ）。	密评机构应将该通道做为网络和通信安全层面的测评对象，进行量化评估和风险评估	若该通道在通过专家评审的密码应用方案中被列为不适用，且方案描述的保护措施与现场情况一致，密评时该通道可做为不适用	密评机构可根据系统情况、该通传输道数据重要性，酌情判定该通道为适用或不适用	若双活机房间使用的为运营商专线，密评机构应将该通道做为网络和通信安全层面的测评对象，进行量化评估和风险评估

4338	多项选择题	对运行在云平台上的云应用进行密评时，根据《商用密码应用安全性评估量化评估规则（2021版）》，以下关于量化评估的说法错误的有（）。	若云平台和云上应用均定级为三级且云平台已通过密评，针对云平台密评时被完全评估的支撑能力，云上应用对应的测评对象必须直接按照云平台的量化评估结果进行量化评价	若云平台和云上应用均定级为三级且云平台已通过密评，针对云平台密评时被完全评估的支撑能力，云上应用对应的测评对象可以判定为不适用	若云平台和云上应用均定级为三级且云平台已通过密评，针对云平台密评时被部分评估的支撑能力，云上应用对应的测评对象的量化评估结论需要结合现场测评和云平台支撑能力说明给定结果	若云平台和云上应用均定级为三级且云平台已通过密评，针对云平台密评时被部分评估的支撑能力，云上应用对应的测评对象可直接取云平台的量化评估结果的一半分数做为量化评价结果
4339	多项选择题	根据《商用密码应用安全性评估量化评估规则（2021版）》，以下说法错误的有（）。	无论哪个安全层面，测评单元的量化评估结果共有{0，0.25，0.5，1}四种情况	在技术要求中，测评单元的量化评估结果介于[0,1]之间，取小数点后4位	在密码应用技术各层面中，测评单元的量化评估结果介于[0,1]之间，取小数点后2位	在密码应用管理各层面中，测评单元的量化评估结果共有{0，0.25，0.5，1}四种情况
4340	多项选择题	某信息系统部署在跨两地的主备机房，关于两个机房物理和环境安全层面的量化评估，根据《商用密码应用安全性评估量化评估规则（2021版）》，以下说法正确的有（）。	应选取两个机房作为测评对象，每项测评单元量化评估结果应为两机房量化评估分数的较低值	应选取两个机房作为测评对象，每项测评单元量化评估结果应为两机房量化评估分数的算术平均值	若已通过专家评估的密码应用方案中将备份机房列为不适用，密评时应选取主机房做为测评对象（备份机房作为不适用），每项测评单元量化评估结果应为主机房对应测评单元的量化结果	应选取两个机房作为测评对象，但应为两个机房分配不同的权重，每项测评单元量化评估结果应为两机房量化评估分数的加权平均值

4341	多项选择题	2021年密评联委会发布的《商用密码应用安全性评估量化评估规则（2021版）》，适用于指导、规范信息系统密码应用的（ ）。	立项、启动	规划、建设	运行、测评	验收、维护
4342	多项选择题	下列说法正确的是（ ）。	《商用密码应用安全性评估量化评估规则（2021版）》应遵循法律法规和最新相关指导性文件的总体要求	根据《商用密码应用安全性评估量化评估规则（2021版）》，强调优先在网络和通信安全层面、设备和计算安全层面和应用和数据安全层面推进密码技术应用	根据《商用密码应用安全性评估量化评估规则（2021版）》，强调特别鼓励使用合规的密码算法/产品/服务	通用要求和密码应用技术要求各安全层面的“密码服务”和“密码产品”指标不单独评价
4343	多项选择题	根据《商用密码应用安全性评估量化评估规则（2021版）》，下列说法正确的是（ ）。	若一个测评对象涉及多个密码算法/产品/服务/密钥，D/A/K都按照最低分值给分	密码应用管理要求不针对各个测评对象的测评结果进行量化评估，其中符合为1分，不符合为0分，部分符合为0.5分	通用要求和密码应用技术要求各安全层面的“密码服务”和“密码产品”指标不单独评价	若某测评对象使用了经检测认证的密码产品且满足相应的密码模块要求，但使用的密码算法/技术不合规，则为部分符合，该测评对象量化评估结果为0.5
4344	多项选择题	某三级信息系统的个人身份信息使用服务器密码机（经检测认证合格）基于SM4算法实现数据存储的机密性保护，而重要业务数据使用了自研且未提供安全性证据的算法实现数据存储的机密性保护，根据《商用密码应用安全性评估量化评估规则（2021版）》，则个人身份信息和重要业务数据的存储机密性量化评估结果可能是（ ）。	0.5，0	1，0	0.25，0.25	0.5，0.25

4345	多项选择题	根据《商用密码应用安全性评估量化评估规则（2021版）》，下列说法正确的是（ ）。	密码应用技术要求和密码应用管理要求的量化评估方法不相同	密码应用技术要求中，某个安全层面的某个测评单元的量化评估结果为该测评单元内所有测评对象测评结果的算术平均值	安全层面的不适用测评指标不参与量化评估过程	对同一个测评指标，二级信息系统和三级信息的指标权重不一定相同
4346	多项选择题	根据《商用密码应用安全性评估量化评估规则（2021版）》，下列说法不正确的是（ ）。	对同一个测评指标，二级信息系统和三级信息的指标权重不一定相同	二级信息系统和三级信息系统（所有安全层面均适用的情况下）安全层面权重一定相同	若该系统物理和环境安全层面、设备和计算安全层面不适用，则该系统其他安全层面总权重之和为75	密码应用管理各安全层面的权重均相同
4347	多项选择题	根据《商用密码应用安全性评估量化评估规则（2021版）》，下列说法不正确的是（ ）。	网络和通信安全、设备和计算安全和应用和数据安全三个层面“访问控制信息完整性”量化评估权重相同	若信息系统未制定密码应用方案，则可判定该系统建设运行层面各测评单元量化评估分值一定为0	若信息系统未制定密码应用方案，已知信息系统于2021年2月1日上线运行，则该系统建设运行中“投入运行前进行密码应用安全性评估”量化评估分值为1	若信息系统测评时发现，其使用的服务器密码机采购时间在商用密码产品认证证书的有效期内，但测评时该证书已过期，则对测评单元评估时，K为×

4348	多项选择题	某三级信息系统应用和数据安全层面测评过程中发现，用户身份鉴别数据（即用户口令）和重要业务数据均通过调用服务器密码机（具有二级商密产品认证证书）进行保护，使用SM3带盐杂凑和HMAC-SM3对身份鉴别数据进行存储机密性保护和存储完整性保护，使用SM4-CBC、SM3算法实现重要业务数据存储机密性和存储完整性保护，则根据《商用密码应用安全性评估量化评估规则（2021版）》，以下说法正确的是（ ）。	重要业务数据存储机密性和存储完整性，量化评估分值相同	重要业务数据存储机密性和存储完整性，量化评估分值不相同	若该系统应用层仅涉及身份鉴别数据、重要业务数据，则数据存储机密性测评单元的量化评估分值为0.5	若该系统应用层仅涉及这两类关键数据，则数据存储完整性测评单元的量化评估分值为0.5
4349	多项选择题	在测评某三级信息系统应用和数据安全层面重要数据存储时发现，该系统个人敏感信息使用SM4-GCM算法算法实现数据存储保护，重要业务数据使用AES-256、HMAC-SHA-256算法实现数据存储保护，且所有密码算法均通过调用具有二级商密产品认证证书的密码设备实现，根据《商用密码应用安全性评估量化评估规则（2021版）》，下列说法不正确的是（ ）。	该系统应用和数据安全层面重要数据存储机密性测评单元分值为0.75	该系统应用和数据安全层面重要数据存储完整性保护测评单元分值为0.25	该系统应用和数据安全层面重要数据存储机密性和完整性保护两个测评单元分值不同	若信息系统改用一级商密产品认证证书的密码设备实现重要数据存储的机密性和完整性保护，则量化评估分值不变
4350	多项选择题	在对某三级信息系统设备和安全层面“身份鉴别”进行测评时，该系统三台操作系统和硬件型号均相同的服务器密码机分值分别为0.25、0.5、0，根据《商用密码应用安全性评估量化评估规则（2021版）》，以下说法正确的是（ ）。	三台服务器密码机可能均具有商用密码产品认证证书	三台服务器密码机可能均不具有商用密码产品认证证书	三台密码机作为同一测评对象时的分值为0	三台密码机作为同一测评对象时的分值为0.5

4351	多项选择题	某三级信息系统在测评过程中发现物理和环境安全层面不适用，网络和通信安全层面分值为0.75，设备和计算安全层面分值为0.6，应用和数据安全层面分值为0.325，根据《商用密码应用安全性评估量化评估规则（2021版）》，以下说法不正确的是（ ）。	如果安全管理四个层面分值均为1，该系统量化评估分值为60.75	安全管理四个层面分值均为1，该系统量化评估分值为67.50	若该系统安全管理所有层面得分均为0，该系统量化评估分值为30.75	若该系统安全管理所有层面得分均为0，该系统量化评估分值为37.50
4352	多项选择题	根据《商用密码应用安全性评估量化评估规则（2021版）》，以下（ ）情况下，测评对象的量化结果最多为0.5。	在网络边界部署采用具有密码产品认证证书的VPN设备（满足密码模块二级要求），并使用ECC_SM4_SM3套件	在网络边界部署采用具有密码产品认证证书的VPN设备（满足密码模块二级要求），并使用TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256套件	在三级系统中，在网络边界部署相应的安全模块（满足密码模块一级要求），并使用ECC_SM4_SM3套件	在网络边界部署未经检测认证的VPN设备，并使用TLS 1.2 协议
4353	多项选择题	已知应急处置安全层面所有测评单元的结果没有不符合，根据《商用密码应用安全性评估量化评估规则（2021版）》，则该安全层面可能的得分为（ ）。	0.2500	0.5000	0.6458	0.8542
4354	多项选择题	根据《商用密码应用安全性评估量化评估规则（2021版）》，在某次测评中，物理和环境安全层面被列为不适用，以下（ ）是可能发生的。	该系统最终得分大于90分	该系统最终测评结论为不符合	该系统最终测评结论为符合	该安全层面属于密码应用技术要求维度
4355	多项选择题	根据《商用密码应用安全性评估量化评估规则（2021版）》，量化评估计算过程中需要考虑的量化内容包括（ ）。	各测评对象的测评结果	测评单元的测评结果	安全层面的测评结果	整体测评结果

4356	多项选择题	根据《商用密码应用安全性评估量化评估规则（2021版）》，对于密码技术要求的量化规则，以下说法正确的是（ ）。	只有DAK全部符合的测评对象得分为1分	密码使用有效，具备安全的密钥管理机制，但使用的密码算法/技术不符合法律法规的规定和密码相关国家标准、行业标准的有关规定的得分为0.5分	密码使用有效，但使用的密码算法/技术不符合法律法规的规定和密码相关国家标准、行业标准的有关规定，相关的密钥管理机制存在问题得分为0.5分	密码使用有效，使用的密码算法/技术符合法律 法规的规定和密码相关国家标准、行业标准的 有关规定，相关的密钥管理机制存在问题判定为0分
4357	多项选择题	根据《商用密码应用安全性评估量化评估规则（2021版）》，对测评对象的测评结果量化评估规则，以下说法错误的是（ ）。	通用要求和密码应用技术要求各安全层面的“密码服务”和“密码产品”指标需单独评价	密码技术要求和应用管理要求都需要对各个测评对象的测评结果进行量化评估	密码技术要求和应用管理要求的分值取值都是{0, 0.25, 0.5,1}	密码技术要求中对各测评对象符合性表述均为符合、部分符合、不符合
4358	多项选择题	根据《商用密码应用安全性评估量化评估规则（2021版）》，对测评对象的测评结果量化评估规则，以下说法正确的是（ ）。	在密码技术要求测评过程中，对于单个测评对象对应的多个实体按照每个实体的DAK的算术平均计算测评对象值	在密码技术要求测评过程中，对于单个测评对象涉及多个实体，按照多个实体的DAK最小值作为测评对象值	使用的密码服务是否安全直接影响DAK的A的符合性判定	密码应用管理要求不对各个测评对象的测评结果进行量化评估
4359	多项选择题	根据《商用密码应用安全性评估量化评估规则（2021版）》，对测评单元的测评结果量化评估规则，以下说法正确的是（ ）。	密码应用技术要求中，测评单元的量化评估结果为该测评单元内所有测评对象测评结果的算术平均值	密码应用技术要求中，测评单元的量化评估结果需要保留小数点后4位	密码应用管理要求的测评单元得分为各测评对象的算术平均值	密码应用管理要求的符合性判定需要根据GM/T 0115给出判定结果

4360	多项选择题	根据《商用密码应用安全性评估量化评估规则（2021版）》，对安全层面的测评结果量化评估规则，以下说法不正确的是（ ）。	密码应用技术要求中，安全层面的量化评估结果为层面内各测评单元的算术平均值	密码应用管理要求的安全层面得分为各测评单元的算术平均值	密码应用技术要求中，安全层面的量化评估结果需要保留小数点后2位	某测评指标不适用，则该安全层面的得分为0
4361	多项选择题	根据《商用密码应用安全性评估量化评估规则（2021版）》，对整体结果量化评估规则，以下说法正确的是（ ）。	密码应用技术要求中，最终的量化评估结果为各安全层面的加权平均值	若某个安全层面的大部分测评指标都不适用，则该安全层面不参与量化评估过程	密码应用技术要求中，安全层面的量化评估结果需要保留小数点后4位	在计算整体结果量化过程中，作为分母的权重值总和总是100分
4362	多项选择题	根据《商用密码应用安全性评估量化评估规则（2021版）》，对最终的结论，以下说法正确的是（ ）。	信息系统的最终结论需要同时参考量化评估的结果和风险判定结果	对于分值大于阈值分的系统，如果经风险评估发现存在风险即判定为不符合	对于分值小于阈值分的系统或存在高风险的系统，最终结论都是不符合	只有整体量化评估结果为 100 分的系统才能判定最终结论为符合
4363	多项选择题	对于某个三级系统，已知安全管理要求中，管理制度、人员管理、建设运行、应急处置的得分均为0.5，根据《商用密码应用安全性评估量化评估规则（2021版）》，以下（ ）是可能出现且整体结论正确的。	物理和环境安全、网络和通信安全、设备和计算安全、应用和数据安全分别为不适用、不适用、不适用、0.4，总分为45.00分	物理和环境安全、网络和通信安全、设备和计算安全、应用和数据安全分别为不适用、不适用、不适用、0.4，总分为27分	物理和环境安全、网络和通信安全、设备和计算安全、应用和数据安全分别为不适用、0.6、不适用、0.4，总分为48.75分	物理和环境安全、网络和通信安全、设备和计算安全、应用和数据安全分别为0.4、不适用、0.4、0，总分为39.00分
4364	多项选择题	根据《商用密码应用安全性评估量化评估规则（2021版）》，下列说法正确的是（ ）。	密码应用管理要求不针对各个测评对象的测评结果进行量化评估	《商用密码应用安全性评估量化评估规则（2021版）》适用于指导、规范信息系统密码应用的规划、建设、运行及测评	信息系统在进行测评过程中，若测评对象的D不符合，则分值为0.5分	信息系统测评结果无高风险且分值不低于阈值，该信息系统的测评结果不一定为基本符合

4365	多项选择题	对于某个三级信息系统，在应用和数据安全层面测评过程中，发现设备的登录采用了WEB登录方式，登录界面需要输入用户名+口令，口令经过加盐并利用SM3做杂凑，根据《商用密码应用安全性评估量化评估规则（2021版）》，则以下说法正确的是（ ）。	“身份鉴别”的量化结果分别为 0	“身份鉴别”的量化结果分别为 0.25	“重要数据传输机密性”的量化结果为0.5	“重要数据存储机密性”的量化结果为1
4366	多项选择题	根据《商用密码应用安全性评估量化评估规则（2021版）》，对三级系统，各安全层面权重值正确的是（ ）。	物理和环境安全层面权重为10	网络和通信安全层面权重为15	设备和计算安全层面权重为20	应用和数据安全层面权重为30
4367	判断题	若某测评指标不适用，根据《商用密码应用安全性评估量化评估规则（2021版）》，则该安全层面不参与量化评估过程。	正确	错误		
4368	判断题	若某个安全层面的所有测评指标都不适用，根据《商用密码应用安全性评估量化评估规则（2021版）》，则该安全层面得分为0。	正确	错误		
4369	判断题	若某个安全层面的所有测评指标都不适用，根据《商用密码应用安全性评估量化评估规则（2021版）》，则该安全层面不参与量化评估过程。	正确	错误		
4370	判断题	若某二级被测信息系统整体量化评估结果为83.26，根据《商用密码应用安全性评估量化评估规则（2021版）》，则可直接判定被测信息系统密评结论为“基本符合”。	正确	错误		
4371	判断题	某第二级信息系统密评时，若“应急处置”中“事件处置”测评指标做为适用，根据《商用密码应用安全性评估量化评估规则（2021版）》，则“事件处置”测评指标应参与量化评估。	正确	错误		

4372	判断题	根据《商用密码应用安全性评估量化评估规则（2021版）》，在密码应用管理要求中，部分符合的测评单元得分一定为0.5分。	正确	错误		
4373	判断题	根据《商用密码应用安全性评估量化评估规则（2021版）》，在密码应用技术要求中，部分符合的测评单元得分一定为0.5分。	正确	错误		
4374	判断题	根据《商用密码应用安全性评估量化评估规则（2021版）》，各安全层面的测评结果量化评估结果，应四舍五入取小数点后4位。	正确	错误		
4375	判断题	GB/T 39786规定的第一级信息系统密码应用要求中无“视频记录数据存储完整性”，因此针对第一级信息系统进行量化评估时，根据《商用密码应用安全性评估量化评估规则（2021版）》，该指标不参与量化评估过程。	正确	错误		
4376	判断题	GB/T 39786规定的第二级信息系统密码应用要求中，“网络边界访问控制信息完整性”应用要求为“可”，因此针对第二级信息系统进行量化评估时，根据《商用密码应用安全性评估量化评估规则（2021版）》，该指标一定不参与量化评估过程。	正确	错误		
4377	判断题	根据《商用密码应用安全性评估量化评估规则（2021版）》，低于100分、不低于阈值（目前是60分），且经风险评估发现没有高风险，则判定被测信息系统“基本符合”。	正确	错误		
4378	判断题	若某信息系统管理安全层面的所有指标都不适用，根据《商用密码应用安全性评估量化评估规则（2021版）》，则整体量化评估结果满分不足100分。	正确	错误		

4379	判断题	若信息系统中某测评单元不适用，根据《商用密码应用安全性评估量化评估规则（2021版）》，则整体量化评估结果满分不足100分。	正确	错误		
4380	判断题	若某安全层面的所有指标都不适用，根据《商用密码应用安全性评估量化评估规则（2021版）》，则该安全层面不影响整体量化评估结果。	正确	错误		
4381	判断题	在判定D、K安全三个维度时，根据《商用密码应用安全性评估量化评估规则（2021版）》，应进行综合考虑和独立判定。	正确	错误		
4382	判断题	在判定D、K安全三个维度时，根据《商用密码应用安全性评估量化评估规则（2021版）》，均进行独立判定。	正确	错误		
4383	判断题	若一个信息系统测评完成后，分值为60分，且无高风险，根据《商用密码应用安全性评估量化评估规则（2021版）》，则可判定该系统的测评结论为“符合”。	正确	错误		
4384	判断题	《商用密码应用安全性评估量化评估规则（2021版）》中的原则包括优先在设备和计算安全、应用和数据安全层面推进密码技术应用。	正确	错误		
4385	判断题	根据《商用密码应用安全性评估量化评估规则（2021版）》，通用要求和密码应用技术要求各安全层面的“密码服务”和“密码产品”指标均应单独评价。	正确	错误		
4386	判断题	根据《商用密码应用安全性评估量化评估规则（2021版）》，针对三级信息系统，设备和计算安全层面、应用和数据安全层面“重要信息资源安全标记完整性”的指标权重是一样的。	正确	错误		

4387	判断题	《商用密码应用安全性评估量化评估规则（2021版）》中测评单元的测评结果量化评估规则，针对密码应用技术要求和密码应用管理要求的判定规则完全相同。	正确	错误		
4388	判断题	根据《商用密码应用安全性评估量化评估规则（2021版）》，针对三级信息系统，在量化评估的过程中，安全管理要求所有测评单元的指标权重一定为0.7或1。	正确	错误		
4389	判断题	根据《商用密码应用安全性评估量化评估规则（2021版）》，三级信息系统和四级信息系统在安全管理要求的四个安全层面的指标权重均一致。	正确	错误		
4390	判断题	根据《商用密码应用安全性评估量化评估规则（2021版）》，若信息系统存在特殊指标项，则该特殊指标不参与量化评估过程。	正确	错误		
4391	判断题	某三级信息系统用户通过智能密码钥匙（具有二级商密产品认证证书），通过和数据库比对智能密码钥匙证书字符串信息的方式实现身份鉴别，根据《商用密码应用安全性评估量化评估规则（2021版）》，则该测评对象分值为0.5。	正确	错误		
4392	判断题	某二级信息系统使用具有商密产品认证证书的密钥管理系统（软件），且进行了正确的部署，根据《商用密码应用安全性评估量化评估规则（2021版）》，密钥管理系统所运行的服务器在设备和计算安全层面“日志记录完整性”量化评估分值一定为1分。	正确	错误		

4393	判断题	某第三级信息系统普通用户使用智能密码钥匙（具有二级商密产品认证证书）进行身份鉴别，但未使用获得电子认证服务密码使用许可证的机构颁发的数字证书，根据《商用密码应用安全性评估量化评估规则（2021版）》，量化评估时，K为不符合。	正确	错误		
4394	判断题	针对信息系统设备和安全层面“日志记录完整性”，某信息系统有三台操作系统和硬件型号均相同的应用服务器，量化评估后分值分别为0.25、0.5、0.25，根据《商用密码应用安全性评估量化评估规则（2021版）》，则这三台应用服务器作为一个测评对象量化评估分值为0.3333。	正确	错误		
4395	判断题	若某个安全层面的部分测评指标不适用，根据《商用密码应用安全性评估量化评估规则（2021版）》，则该安全层面不参与量化评估过程。	正确	错误		
4396	判断题	根据《商用密码应用安全性评估量化评估规则（2021版）》，密码应用管理要求不针对各个测评对象的测评结果进行量化评估。	正确	错误		
4397	判断题	整体量化评估结果为 100 分，根据《商用密码应用安全性评估量化评估规则（2021版）》，则判定被测信息系统的测评结果为“符合”。	正确	错误		
4398	判断题	整体量化评估结果低于 100 分但不低于阈值，根据《商用密码应用安全性评估量化评估规则（2021版）》，则判定被测信息系统测评结果为“基本符合”。	正确	错误		

4399	判断题	整体量化评估结果低于阈值，或经风险评估发现存在高风险，根据《商用密码应用安全性评估量化评估规则（2021版）》，则判定被测信息系统不符合GB/T39786相应等级要求。	正确	错误		
4400	判断题	根据《商用密码应用安全性评估量化评估规则（2021版）》，经认证合格的密码产品，在应用和数据层面测评过程中可直接对DAK中的K直接判定为“符合”。	正确	错误		
4401	判断题	根据《商用密码应用安全性评估量化评估规则（2021版）》，若一个测评对象，涉及多个密码算法/产品/服务/密钥，D/A/K按照平均值给分。	正确	错误		
4402	判断题	某个三级系统在网络和通信安全层面测评中，某个测评单元存在4个测评对象，分别得分为1、1、0.5、0.5，根据《商用密码应用安全性评估量化评估规则（2021版）》，则该测评单元得分为0.75分。	正确	错误		
4403	判断题	某个三级系统在网络和通信安全层面测评中，某个测评单元存在3个测评对象，分别得分为1、0.5、0.5，根据《商用密码应用安全性评估量化评估规则（2021版）》，则该测评单元得分为0.5分。	正确	错误		
4404	判断题	已知某系统管理制度的6项测评指标得分分别为0.5、0.5、0.5、0.5、0.5、0.5，对应权重为1、0.7、0.7、0.7、0.7、0.7，根据《商用密码应用安全性评估量化评估规则（2021版）》，则该安全层面得分为0.5000。	正确	错误		

4405	判断题	《商用密码应用安全性评估量化评估规则（2021版）》中某层面的不适用项数量不会影响其他安全层面得分。	正确	错误		
4406	判断题	《商用密码应用安全性评估量化评估规则（2021版）》中不适用项对应的权重指标在计算过程中不计入分值。	正确	错误		
4407	判断题	《商用密码应用安全性评估量化评估规则（2021版）》中对于不同的等级同一测评项的指标权重总是相同。	正确	错误		
4408	判断题	《商用密码应用安全性评估量化评估规则（2021版）》中不同的安全层面权重分值相同。	正确	错误		
4409	判断题	根据《商用密码应用安全性评估量化评估规则（2021版）》，在测评过程中，重要数据传输机密性与传输完整性两个指标涉及的测评对象数量可以是不同的。	正确	错误		
4410	判断题	某信息系统测评过程中，提供了管理系统人员的相关培训制度文件，根据《商用密码应用安全性评估量化评估规则（2021版）》，在人员管理层面的“定期进行安全岗位人员考核”一项得分为1分。	正确	错误		
4411	判断题	某信息系统，投入运营时间为2019年10月，该系统无法提供密码应用方案，但系统制定了密码应用改造方案并经过评审，根据《商用密码应用安全性评估量化评估规则（2021版）》，建设运行层面的“制定密码应用方案”得分为0分。	正确	错误		

4412	判断题	某个三级系统使用SM3算法保护系统数据的传输完整性，根据《商用密码应用安全性评估量化评估规则（2021版）》，应用和数据安全层面中重要数据传输完整性的量化得分为1分。	正确	错误		
4413	判断题	某个四级系统在网络间采用了SSL VPN，通过网络抓包发现服务器端发送了国密数字证书，客户端未发送任何数字证书，根据《商用密码应用安全性评估量化评估规则（2021版）》，网络和通信安全层面的身份鉴别项，得分为1分。	正确	错误		
4414	判断题	根据《商用密码应用安全性评估量化评估规则（2021版）》，安全层面的测评结果不需要保留小数。	正确	错误		
4415	判断题	某三级信息系统用户口令存储时，先使用DES算法加密后再使用SM4算法加密，使用的密码产品具有二级密码模块认证证书，根据《商用密码应用安全性评估量化评估规则（2021版）》，口令做为测评对象在“重要数据存储机密性”测评单元的量化评估结果为1分。	正确	错误		
4416	判断题	某三级信息系统用户口令传输时，用户可选择使用MD5算法或者SM3算法进行杂凑后，将杂凑结果发至服务端校验，服务器根据用户选取的算法类型使用MD5或者SM3算法进行校验，客户端使用的密码产品具有二级认证证书，根据《商用密码应用安全性评估量化评估规则（2021版）》，口令做为测评对象在“重要数据传输机密性”测评单元的量化评估结果为1分。	正确	错误		

4417	单项选择题	依据《信息系统密码应用高风险判定指引》，信息系统应用和数据层面，未采用密码技术对登录用户进行身份鉴别时，可以采用的缓解措施有（）。	安排专人值守	部署视频监控	部署入侵检测系统	采用基于特定识别技术进行身份鉴别，如设备指纹、生物指纹和第三方身份鉴别服务等
4418	单项选择题	密评过程中，如果遇到《信息系统密码应用高风险判定指引》没有描述的风险判定情况，那么测评人员应（ ）。	结合实际情况进行综合判定风险	判定为高风险	判定为中风险	判定为低风险
4419	单项选择题	依据《信息系统密码应用高风险判定指引》，信息系统中使用的密码产品或服务可能引起高风险的是（ ）。	使用自实现且能够提供安全证明的密码产品	使用的密码产品存在高危漏洞	密码产品的使用符合国家密码主管部门的管理要求和标准规范的要求	密码服务提供商具有国家密码管理部门的相关资质
4420	单项选择题	在《信息系统密码应用高风险判定指引》中，对安全接入认证问题的风险判定适用于（ ）。	第一级信息系统	第二级信息系统	第三级信息系统	第四级信息系统
4421	单项选择题	依据《信息系统密码应用高风险判定指引》，以下不存在缺陷或没有安全问题警示的密码技术是（）。	SSH 1.0	TLS 1.3	SSL 2.0	SSL 3.0
4422	单项选择题	某系统采用了未经安全性论证的密码通信协议，依据《信息系统密码应用高风险判定指引》，则该情况属于哪种风险（）。	密码算法层面 的风险	密码产品层面的风险	密码技术层的面风险	密码服务层面的风险
4423	单项选择题	在《信息系统密码应用高风险判定指引》中，关于指标“信息系统中使用的密码产品、密码服务应符合法律法规的相关要求”，主要是针对（）系统提出的。	第二级以上	第三级以上	所有级别	第三级
4424	单项选择题	依据《信息系统密码应用高风险判定指引》中，网络通信过程中重要数据的机密性可以从（）层面进行缓解，从而降低安全风险。	设备和计算安全	应用和数据安全	物理和环境安全	安全管理制度

4425	单项选择题	依据《信息系统密码应用高风险判定指引》，网络和通信安全层面如果未采用基于（ ）的数字签名机制等密码技术对通信实体进行身份鉴别，可能会导致信息系统面临高风险。	公钥密码算法	对称密码算法	密码杂凑算法	标识算法
4426	单项选择题	依据《信息系统密码应用高风险判定指引》，网络和通信安全层面如果未采用基于对称密码算法或（ ）的消息鉴别码（MAC）机制等密码技术对通信实体进行身份鉴别，可能会导致信息系统面临高风险。	密码杂凑算法	生物特征	祖冲之密码算法	公钥密码算法
4427	单项选择题	依据《信息系统密码应用高风险判定指引》，没有采用密码技术保证远程通道管理安全的情况下，信息系统为降低安全风险，可采用的缓解措施包括：搭建与业务网络（ ）隔离，并采取相应的安全防护措施的专用管理网络。	逻辑	物理	区域	边界
4428	单项选择题	依据《信息系统密码应用高风险判定指引》，应用系统在身份鉴别方面，可能存在高风险的是（ ）。	使用了基于国产密码算法的USBKey实现用户身份的鉴别	采用的密码产品具有商用密码产品认证证书	用户身份真实性的密码技术实现机制正确且有效	用户口令使用SM3密码算法处理后存储
4429	单项选择题	依据《信息系统密码应用高风险判定指引》，应用和数据安全层面没有采用密码技术保证用户身份鉴别安全的情况下，不属于降低信息系统安全风险可采用的缓解措施是（ ）。	动态口令机制	设备指纹	生物指纹	第三方身份鉴别服务
4430	单项选择题	依据《信息系统密码应用高风险判定指引》，能够最有效缓解应用和数据层面重要数据存储机密性安全风险的方式是（ ）。	使用MD5算法实现重要数据存储机密性保护	使用SM4算法实现重要数据存储机密性保护	使用SM3算法实现重要数据存储机密性保护	使用SHA-256算法实现重要数据存储机密性保护

4431	单项选择题	依据《信息系统密码应用高风险判定指引》，在没有采用密码技术保证进入机房人员身份鉴别安全的情况下，以下能够降低安全风险的措施是（）。	采用用户名+口令+ID卡方式鉴别进入人员身份	人员信息自行登记后进入	机房出入口配备专人值守并进行登记，且采用视频监控系统进行实时监控	机房禁止外部人员进入
4432	单项选择题	依据《信息系统密码应用高风险判定指引》，以下对于通用要求中“密码技术”描述正确的是（）。	该要求适用级别为一级到四级信息系统	若采用OpenSSL协议库实现TLS，则一定不会导致高风险	指标要求为“信息系统中使用的密码技术应遵循密码相关国家标准和行业标准”	若使用TLS 1.1,则一定会导致高风险
4433	单项选择题	依据《信息系统密码应用高风险判定指引》，以下对通用要求中“密码产品”描述不正确的是（）。	使用了具有电子认证服务密码使用许可证的CA机构签发是数字证书，一定不会导致高风险	使用自实现且未提供安全性证明的密码产品，可能会导致高风险	使用存在高危安全漏洞的公开算法库，可能会导致高风险	三级信息系统中，使用了安全等级二级的密码产品，也可能会导致高风险
4434	单项选择题	对测评单元“重要数据存储完整性”的测评结果如果为“部分符合”，依据《信息系统密码应用高风险判定指引》，以下哪些情况可以缓解风险（）。	应用系统具有符合要求的身份鉴别措施，保证只有授权人员才能访问应用系统的重要数据，且定期对重要数据进行备份	对数据进行加密存储保护	定期对重要数据进行备份	对数据进行加密传输保护
4435	单项选择题	在设备和计算安全层中，依据《信息系统密码应用高风险判定指引》，能够降低服务器身份鉴别安全风险的措施是（）。	采用设备指纹方式登录服务器	采用手机短信验证码方式登录服务器	登录堡垒机后，再输入用户名+口令的方式，登录服务器	采用进入机房，本地运维的方式进行服务器管理

4436	单项选择题	SSL VPN设备采用HTTPS协议进行管理（TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384），依据《信息系统密码应用高风险判定指引》，对远程管理通道安全测评指标的结果判定最合理的是（）。	符合	部分符合	不适用	不符合
4437	单项选择题	数据库服务器采用SSH协议进行远程管理，协议中使用非国密算法保障远程管理通道的安全，且经漏洞扫描发现SSH协议存在高风险漏洞。依据《信息系统密码应用高风险判定指引》，以下对远程管理通道安全测评指标结果判定正确的是（）。	0.5分	0分	存在高风险安全问题	存在低风险安全问题
4438	单项选择题	根据《信息系统密码应用高风险判定指引》，对采用密码技术实现数据完整性和机密性保护，说法错误的是（）。	业务系统中对身份证号、手机号等重要个人信息不应采用杂凑算法保证其机密性	数据完整性保护主要基于杂凑算法或数字签名算法实现	数据机密性主要基于对称或非对称密码算法实现	数据完整性和机密性应使用相同的密码算法实现
4439	单项选择题	根据《信息系统密码应用高风险判定指引》，通常使用（）方法来实现数据原发行为的不可否认性和数据接收行为的不可否认性。	加密	时间戳	数字签名	手写签字
4440	单项选择题	依据《信息系统密码应用高风险判定指引》，（）是建立评估对象所需密钥管理策略和密钥管理规则的主要依据。	评审通过的密码应用方案	系统安全性设计方案	系统建设实施方案	项目立项报告

4441	单项选择题	某面向公众的三级门户网站系统通过部署经检测认证合格的安全网关（密码模块二级），使用TLS _ECDHE_ RSA_WITH _AES_ 256_ GCM_ SHA384密码算法套件，实现通信过程中重要数据的机密性和完整性保护，则根据《信息系统密码应用高风险判定指引》，以下对该密码技术实现方式的风险分析描述正确的是（ ）。	使用的密码算法可能不合规	存在密钥被非法授权篡改，或密钥与实体之间的关联关系被非法授权篡改的风险	密钥质量随机性不好，存在被攻击者猜测的风险	存在通信数据在信息系统外部被截取、篡改的风险
4442	单项选择题	根据《信息系统密码应用高风险判定指引》，网络和通信安全层面的身份鉴别高风险适用于以下信息系统（ ）。	一级信息系统	二级信息系统	三级及以上级别信息系统	二级及以上级别信息系统
4443	单项选择题	依据《信息系统密码应用高风险判定指引》，以下关于网络和通信安全层面“通信过程中重要数据机密性”风险缓解措施有效的是（ ）。	在“应用和数据安全”层面仅针对信息系统部分重要数据传输采用符合要求的密码技术进行机密性保护，且加密后的数据流能够覆盖网络通信信道	在“应用和数据安全”层面对信息系统所有需要保护的重要数据传输采用符合要求的密码技术进行机密性保护，且加密后的数据流能够覆盖网络通信信道	针对内网访问的信息系统，因不涉及互联网数据传输，所以可以降低网络和通信安全层面“通信过程中重要数据的机密性”面临的安全风险	通过专线进行数据传输的通道，可以认为专线面临的安全风险可控，能够降低其面临的安全风险
4444	单项选择题	依据《信息系统密码应用高风险判定指引》，密钥更新环节可能会对密钥安全造成安全隐患的是（ ）。	按照制定的密钥生命周期的安全管理策略执行	未建立密钥已泄露或存在泄露风险时的密钥更新机制	在更新密钥过程中，填写相关表格进行记录	密钥定期备份
4445	多项选择题	依据《信息系统密码应用高风险判定指引》，网络和通信安全层面如果通信实体身份真实性的密码技术实现机制（ ）或无效，可能会导致信息系统面临高风险。	不科学	不安全	不完整	不正确

4446	多项选择题	依据《信息系统密码应用高风险判定指引》，以下对通用要求“密码算法”描述不正确的是（）。	指标要求是“信息系统中使用的密码算法应符合密码相关国家标准、行业标准的有关要求”	对所有不同安全等级的信息系统均适用	存在可能的缓解措施	若信息系统中采用OpenSSL算法库实现AES，为信息系统提供加密保护，则会导致高风险
4447	多项选择题	依据《信息系统密码应用高风险判定指引》，以下对通用要求中“密码算法”的描述正确的是（）。	采用DES算法提供数据加密，则很可能导致高风险	采用SHA-1提供口令存储完整性保护，则很可能导致高风险	采用自行设计的数据处理算法，达到将数据不可读的目的，则该算法依然可能导致高风险	采用MD5 with RSA2048进行数字签名，不会导致高风险
4448	多项选择题	在《信息系统密码应用高风险判定指引》中，以下属于不安全的密码算法是（）。	SM2	SHA-1	RSA-1024	MD5
4449	多项选择题	在《信息系统密码应用高风险判定指引》中,以下属于密码算法安全问题的是（）。	采用了安全强度不够的密码算法	自行设计的密码算法	采用未经安全性论证的密码算法	采用了符合法律、法规规定和密码相关国家标准、行业标准有关要求的算法
4450	多项选择题	某单位管理员远程登录服务器时，采用密码协议保证远程管理通道安全，依据《信息系统密码应用高风险判定指引》，避免带来高风险，以下可能采用的协议包括（）。	SSH 2.0	SSL 2.0	SSL 3.0	TLS 1.2
4451	多项选择题	在《信息系统密码应用高风险判定指引》中，未涉及的安全问题场景，以下判定其风险程度的做法正确的是（）。	结合实际场景客观判断	无需关注	需分析考虑是否对其造成严重的安全隐患	直接判定为中或低风险
4452	多项选择题	在《信息系统密码应用高风险判定指引》中，对高风险判定，从（）方面进行了描述。	指标要求	适用范围	安全问题	可能的缓解措施和风险评价

4453	多项选择题	密评过程中发现的问题，在《信息系统密码应用高风险判定指引》中没有相关描述的，仍需从（）方面核查该问题是否存在风险。	密码算法	密码技术	密码产品	密码服务
4454	多项选择题	依据《信息系统密码应用高风险判定指引》，采用密码技术对重要区域进入人员进行身份鉴别的措施可包括（）。	采用动态口令机制	基于对称密码算法或密码杂凑算法的消息鉴别码（MAC）机制	基于公钥密码算法的数字签名机制	基于生物特征识别
4455	多项选择题	依据《信息系统密码应用高风险判定指引》，属于物理和环境安全层面身份鉴别方面引发的安全问题的是（）。	对进出机房人员采用的身份鉴别类产品不符合密码产品相关要求	对进出机房人员的身份鉴别机制无效	机房未采用视频监控系统	对进出机房人员未采用基于密码技术的身份鉴别措施
4456	多项选择题	在《信息系统密码应用高风险判定指引》中，对网络和通信安全层面的通信实体进行身份鉴别时，引发高风险的原因可能是（）。	密码技术实现机制不正确或无效	未采用基于消息鉴别码（MAC）的机制	未采用数字签名机制	采用的密码产品未获得商用密码产品认证证书
4457	多项选择题	某信息系统的用户仅使用“用户名+口令”方式进行登录系统，根据《信息系统密码应用高风险判定指引》，以下（）措施可以缓解这种登录方式带来的风险	设备指纹	人脸识别	第三方身份鉴别服务	指纹识别
4458	多项选择题	设备指纹是指可以用于标识出该设备的设备特征或者独特的设备标识，用于区分和识别不同的设备。按照《信息系统密码应用高风险判定指引》的规定，设备指纹因子包括（）。	计算机的操作系统类型	设备的硬件ID	手机的IMEI	电脑的网卡MAC地址

4459	多项选择题	用户先通过SSL VPN接入信息系统内网，然后再通过浏览器登录系统内部应用。根据《信息系统密码应用高风险判定指引》，以下对该系统风险缓解的描述，合理的有（ ）。	用户通过使用智能密码钥匙登录SSL VPN，经测评为符合；因此，该应用的用户角色的“身份鉴别”指标的风险可以适当降低	如果SSL VPN所涉及的通信信道对应的“网络和应用安全”层面的“身份鉴别”指标均为符合，那么应用和数据安全层面的“身份鉴别”指标的风险可以适当降低	如果SSL VPN所涉及的通信信道相应的“网络和应用安全”层面的“通信过程中重要数据的机密性”指标均为符合，那么应用和数据安全层面的“重要数据传输机密性”指标的风险可以适当降低	《信息系统密码应用高风险判定指引》不涉及“网络和应用安全”层面的“重要数据传输完整性”指标，因此该指标不会存在高风险
4460	多项选择题	在《信息系统密码应用高风险判定指引》中，以下存储保护方式会导致系统在“重要数据存储完整性”方面存在高危风险的有（ ）。	使用SHA1 With RSA-2048进行数字签名	使用SM3杂凑算法对数据进行杂凑计算，杂凑值与数据一同存放	使用SM4-GCM算法对数据进行加密保护	使用HMAC-SM3对数据进行MAC计算，但是仅截取MAC的8个比特进行使用
4461	多项选择题	在《信息系统密码应用高风险判定指引》中，以下存储保护方式会导致系统在“重要数据存储机密性”方面存在高危风险的有（ ）。	使用DES-CBC进行数字签名	使用SM4-CBC算法加密	使用RSA-1024算法对SM4密钥加密	使用SM4-GCM算法对数据进行加密保护
4462	多项选择题	在《信息系统密码应用高风险判定指引》中，以下实现用户身份真实性的措施，不会带来安全问题的是（ ）。	生物指纹技术	动态口令机制	基于对称密码算法或密码杂凑算法的消息鉴别码（MAC）机制	基于公钥密码算法的数字签名机制
4463	多项选择题	《信息系统密码应用高风险判定指引》中，在应用和数据安全层面，采用以下（ ）措施，可以可缓解系统在用户身份鉴别方面存在的安全风险。	采用设备指纹保证用户身份的真实性	采用生物指纹保证用户身份的真实性	采用第三方身份鉴别服务保证用户身份的真实性	绑定登录用户终端的IP地址

4464	多项选择题	在《信息系统密码应用高风险判定指引》中，使用（ ）身份鉴别方式，可能会触发应用和数据安全层面“身份鉴别”的风险判定。	USB-Key	动态口令机制	短信验证码	邮箱验证码
4465	多项选择题	在《信息系统密码应用高风险判定指引》中，使用（ ）方法不会触发应用和数据层面“重要数据传输机密性”的风险判定。	采用标准tls 1.2协议	基于SM4-CBC对称密码算法	基于SM2非对称密码算法	基于Base64编码的方式
4466	多项选择题	在《信息系统密码应用高风险判定指引》中，（ ）属于应用和数据层面“重要数据存储机密性”的涉及范围。	业务系统采用AES加密存储数据	使用SM3密码算法保存了银行客户的身份证号，以便发给公安系统进行比对	使用HMAC-SM3算法对关键业务数据进行完整性保护	使用SM4算法实现重要数据传输的机密性
4467	多项选择题	依据《信息系统密码应用高风险判定指引》，下列说法错误的是（ ）。	可使用密码杂凑算法的消息鉴别码（MAC）机制解决数据传输机密性的高风险问题	可使用基于公钥密码算法的数字签名机制解决数据存储完整性问题	三级及以上信息系统一定存在不可否认性的高风险问题	使用RSA1024算法可解决重要数据存储机密性问题
4468	多项选择题	依据《信息系统密码应用高风险判定指引》，在应用和数据安全层面，可能存在高风险项的是（ ）。	身份鉴别	重要数据传输机密性	重要数据传输完整性	重要数据存储完整性
4469	多项选择题	依据《信息系统密码应用高风险判定指引》，密评过程中主要关注的管理制度有（ ）。	密码人员管理	密钥管理	建设运行	应急处置
4470	多项选择题	由于密码技术的安全依赖于密钥安全，因此密钥的安全管理是密码技术应用中非常重要的环节，下列属于密钥管理环节的是（ ）。	使用	更新	归档	销毁

4471	多项选择题	依据《信息系统密码应用高风险判定指引》，以下内容可能会给密钥管理带来安全隐患的是（ ）。	未采用通过检测认证合格的随机数发生器生成密钥，且无公开文献和证据证明随机数发生器的合理性和正确性	密钥在不可控的环境中生成	密钥协商之前或协商过程中没有验证对方身份真实性	密钥由具有商用密码认证证书的密码产品产生
4472	多项选择题	依据《信息系统密码应用高风险判定指引》，密钥分发环节可采取的安全措施有（ ）。	使用没有访问控制机制的存储介质（如普通信封、普通U盘）等传输明文密钥	密钥在可控的环境中分发，使用了密码技术保护密钥的机密性和完整性	分发密钥时，一人可领取多段密钥	密钥明文及其组件采用电子邮件、传真、电传、电话等方式直接传递
4473	多项选择题	依据《信息系统密码应用高风险判定指引》，密钥销毁和撤销环节可能会对密钥管理带来安全隐患是（ ）。	不具备密钥在应急情况下的密钥销毁/撤销的机制	未按照设定的安全机制进行密钥销毁/撤销	对于磁记录存储器存储的密钥，简单的删除、清0或写1即可	停止使用的密钥一般不要立即毁掉，而需再保存一段时间然后再毁掉
4474	多项选择题	在《信息系统密码应用高风险判定指引》中，对“通用要求”部分的理解正确的是（ ）。	指标要求来自于GB/T 39786《信息安全技术 信息系统密码应用基本要求》的通用要求部分	描述的内容适用范围是从二级到四级信息系统	不存在可能的缓解措施	若出现相应安全问题的情形，则一定会导致高风险
4475	多项选择题	依据《信息系统密码应用高风险判定指引》，对于通用要求“密码算法”的描述正确的是（ ）。	描述的内容适用范围为所有级别信息系统	RSA（不足2048比特）可能会导致高风险	采用自行设计的密码算法可能会导致高风险	使用MD5杂凑算法可能导致高风险
4476	多项选择题	依据《信息系统密码应用高风险判定指引》，对于通用要求“密码技术”的描述正确的是（ ）。	测评过程中，在该方面若发现问题，存在可能的缓解措施	系统采用了未经安全性论证的密码协议，可能会给系统带来高风险	使用TLS 1.0协议实现对通信信道的保护，可能会导致高风险	信息系统选用密码技术时，需考虑该密码技术是否遵循密码相关国家标准和行业标准

4477	多项选择题	依据《信息系统密码应用高风险判定指引》，对于通用要求“密码算法”的描述不正确的是（ ）。	存在安全问题或安全强度不足的密码算法可能会导致高风险	使用自行设计的密码算法可能会导致高风险	未经安全性论证的密码算法可能会导致高风险	该指标对应的密码算法不仅要符合法律要求，还应遵循国家标准
4478	多项选择题	依据《信息系统密码应用高风险判定指引》，通用要求“密码产品和密码服务”中，密码产品存在可能导致高风险的问题有（ ）。	密码产品在使用时未按照产品的安全策略文档部署和使用	不具有商用密码产品认证证书	密码服务提供商不具有相关资质	密码厂商自研一套软件密码模块，但无法提供该密码产品的安全性证明结论
4479	多项选择题	根据《信息系统密码应用高风险判定指引》，下列属于密钥管理环节的是（ ）。	产生	撤销	备份	恢复
4480	多项选择题	依据《信息系统密码应用高风险判定指引》，某三级信息系统主备机房，采用8位以上的口令，对进入机房的用户进行身份鉴别。以下针对身份鉴别测评指标的符合性判定以及针对问题风险的判定正确的是（ ）。	不符合	高风险	部分符合	中风险
4481	多项选择题	依据《信息系统密码应用高风险判定指引》，某三级信息系统主备机房，采用人脸识别技术对进入机房的用户进行身份鉴别，并在机房出入口配备专人值守，并保留了人员进出记录，以下针对身份鉴别测评指标的符合性判定以及针对问题风险的判定正确的是（ ）。	不符合	高风险	部分符合	中风险
4482	多项选择题	依据《信息系统密码应用高风险判定指引》，以下措施能够缓解设备和计算安全层面远程管理通道安全测评项的高风险的是（ ）。	采用带外管理的方式对所有设备进行远程管理	所有运维人员均需要通过堡垒机进行身份认证	所有设备均需要运维人员通过SSL VPN设备进行远程管理，且采用的密码技术符合要求	运维人员采用两种身份鉴别措施对设备进行远程管理，其中一种身份鉴别措施为密码技术

4483	多项选择题	根据《信息系统密码应用高风险判定指引》，以下采用的措施对物理和环境安全的身份鉴别，可能带来安全风险的是（ ）。	采用口令方式鉴别进入人员身份	采用ID卡方式鉴别进入人员身份	采用指纹识别方式鉴别进入人员身份	机房采用物理锁方式控制人员进出
4484	判断题	依据《信息系统密码应用高风险判定指引》，若未采用密码技术对重要区域进入人员进行身份鉴别，但基于生物识别技术（如指纹等）保证人员身份真实性，可酌情降低风险等级。	正确	错误		
4485	判断题	根据《信息系统密码应用高风险判定指引》，依据相关密码算法标准自行开发实现的国密算法满足标准要求。	正确	错误		
4486	判断题	根据《信息系统密码应用高风险判定指引》，远程管理设备时，未采用密码技术建立安全的信息传输通道且无缓解措施的情况下，风险分析应判断为高风险。	正确	错误		
4487	判断题	依据《信息系统密码应用高风险判定指引》，在应用和数据安全层面，未采用密码技术对登录用户进行身份鉴别，保证应用系统用户身份的真实性，但基于特定识别技术（如设备指纹、生物指纹、第三方身份鉴别服务等）保证用户身份的真实性，可酌情降低风险。	正确	错误		
4488	判断题	根据《信息系统密码应用高风险判定指引》，在应用和数据安全层面，未采用密码技术保证信息系统应用的重要数据在传输过程中的机密性，可直接判定为高风险问题。	正确	错误		
4489	判断题	根据《信息系统密码应用高风险判定指引》，第二级及以上级别信息系统，未采用密码技术保证信息系统应用的重要数据在存储过程中的完整性，可直接判定为高风险问题。	正确	错误		

4490	判断题	某单位在密码应用改造方案中，采用了自行设计研发的密码算法实现数据的保密性保护，经内部确认该算法比较安全，该算法不会触发高风险判定。	正确	错误		
4491	判断题	根据《信息系统密码应用高风险判定指引》，应确保三级以上的信息系统中使用的密码算法符合法律、法规的规定和密码相关国家标准、行业标准的有关要求，其他级别可酌情考虑。	正确	错误		
4492	判断题	根据《信息系统密码应用高风险判定指引》，若信息系统所使用的密码技术未遵循密码相关国家标准和行业标准，则一定会导致信息系统面临高等级安全风险。	正确	错误		
4493	判断题	根据《信息系统密码应用高风险判定指引》，若信息系统中使用了存在安全问题的密码产品、密码服务，则可通过采取一定的缓解措施来降低可能的风险。	正确	错误		
4494	判断题	某单位在密码改造工作中，采用自实现且未提供安全性证据的密码产品实现数据库的数据存储保密性保护，但考虑到数据仅内网访问，且数据库部署了审计产品，可从一定程度上缓解风险程度。	正确	错误		
4495	判断题	信息系统测评过程中的风险判定只需依据《信息系统密码应用高风险判定指引》所列出的相关安全问题所引发的风险等级做出判断。	正确	错误		
4496	判断题	依据《信息系统密码应用高风险判定指引》，缓解措施是指可以降低威胁利用安全问题导致安全事件发生造成严重程度的安全措施。	正确	错误		

4497	判断题	《信息系统密码应用高风险判定指引》中所涉及的指标要求包括了《信息安全技术 信息系统密码应用基本要求》所有要求项。	正确	错误		
4498	判断题	依据《信息系统密码应用高风险判定指引》，虽未采用密码技术对重要区域进入人员进行身份鉴别，但基于生物识别技术（如指纹等）同样保证了人员身份真实性，可酌情降低风险等级。	正确	错误		
4499	判断题	依据《信息系统密码应用高风险判定指引》，在网络和通信安全中，通信实体身份鉴别方面的高风险问题可以有缓解措施。	正确	错误		
4500	判断题	依据《信息系统密码应用高风险判定指引》，在网络通信过程中，重要数据机密性方面的高风险问题有缓解措施。	正确	错误		
4501	判断题	依据《信息系统密码应用高风险判定指引》，在网络和通信安全中，安全接入认证方面的高风险问题没有缓解措施。	正确	错误		
4502	判断题	《信息系统密码应用高风险判定指引》中，安全接入认证方面的要求适用范围包含三级和四级信息系统。	正确	错误		
4503	判断题	依据《信息系统密码应用高风险判定指引》，设备和计算安全中，身份鉴别方面的高风险问题没有缓解措施。	正确	错误		
4504	判断题	依据《信息系统密码应用高风险判定指引》，设备和计算安全层面的身份鉴别，必须采用密码技术保证用户身份的真实性，没有缓解措施。	正确	错误		

4505	判断题	依据《信息系统密码应用高风险判定指引》，业务系统用户登录时，系统可通过用户名、口令的鉴别方式实现用户身份的鉴别。	正确	错误		
4506	判断题	依据《信息系统密码应用高风险判定指引》，业务用户登录时，可使用基于动态令牌的身份鉴别方式实现用户身份的鉴别，其中采用DES算法生成动态令牌。	正确	错误		
4507	判断题	依据《信息系统密码应用高风险判定指引》，业务用户登录系统时，系统对登录用户仅采用指纹认证的方式进行身份鉴别，由于鉴别过程未采用密码技术实现，则用户身份真实性方面可判定存在高风险问题。	正确	错误		
4508	判断题	依据《信息系统密码应用高风险判定指引》，系统可采用RSA1024密码算法，实现信息系统重要数据在传输过程中的机密性。	正确	错误		
4509	判断题	依据《信息系统密码应用高风险判定指引》，在“网络和通信安全”层面，采用符合要求的密码技术为网络通信信道提供机密性保护，且网络通信信道经评估无高风险，可酌情降低“应用和数据安全”层面未采用密码技术对重要数据进行传输机密性保护的风险等级。	正确	错误		
4510	判断题	依据《信息系统密码应用高风险判定指引》，使用MD5算法实现对重要数据存储完整性保护，可判定为高风险问题。	正确	错误		
4511	判断题	依据《信息系统密码应用高风险判定指引》，未采取密码技术措施实现数据原发行为的不可否认性和数据接收行为的不可否认性，则无其他可能的缓解措施对该问题风险进行缓解。	正确	错误		

4512	判断题	依据《信息系统密码应用高风险判定指引》，现场“对密码关键岗位人员进行上岗培训”测评时，测评人员应核查安全教育和培训计划文档是否具有针对涉及密码应用的操作和管理人员的培训计划，以及开展培训的记录。	正确	错误		
4513	判断题	依据《信息系统密码应用高风险判定指引》，针对存量系统要制定密码应用整改方案，该方案可不进行评审。	正确	错误		
4514	判断题	依据《信息系统密码应用高风险判定指引》，密钥在恢复使用时，在对其他系统缺乏鉴别机制的情况下，可以被导入到其他系统中。	正确	错误		
4515	判断题	依据《信息系统密码应用高风险判定指引》，密码应用安全管理制度描述的内容适用范围是三级及以上级别信息系统。	正确	错误		
4516	判断题	依据《信息系统密码应用高风险判定指引》，在通用要求的“密码技术”方面发现的高风险问题，存在可能的缓解措施。	正确	错误		
4517	判断题	未纳入《信息系统密码应用高风险判定指引》的指标条款，则一定不会导致高风险情形。	正确	错误		
4518	判断题	某三级信息系统采用堡垒机对服务器进行统一运维管理，堡垒机采用用户名+口令方式登录，服务器通过堡垒机采用用户名+口令方式登录，两次身份鉴别措施不相同，则针对“设备和计算安全”层面的身份鉴别测评可以判定系统存在中风险安全问题。	正确	错误		

4519	判断题	按照《信息系统密码应用高风险判定指引》，某信息系统的用户仅使用“用户名+口令”方式进行登录，则“应用和数据安全”层面的“身份鉴别”指标判定为不符合，但是不会存在高危风险。	正确	错误		
4520	判断题	某信息系统改造前，使用DES算法对数据进行加密保护，改造后，新增服务器密码机，使用SM4-GCM对原先DES加密的数据密文进行进一步加密保护。在进行测评时，这种方式一定会导致“重要数据存储机密性”指标存在高危风险。	正确	错误		
4521	判断题	某信息系统在“网络和通信安全”层面对接入的用户设备进行了身份鉴别，但“应用和数据安全”未对用户进行身份鉴别，而是直接使用了“网络和通信安全”层面的“身份鉴别”结果，默认接入的用户可以登录应用。因此，按照《信息系统密码应用高风险判定指引》，“身份鉴别”指标的风险可以进行适当降低；如果风险降为“低”，则该指标结果可以弥补为“符合”。	正确	错误		
4522	判断题	用户登录某信息系统的方式为“用户名+口令”方式，口令通过SSL VPN加密传输保护。在进行测评时这种方式不会导致“身份鉴别”指标存在高危风险。	正确	错误		

4523	判断题	某信息系统为用户提供期货交易服务，交易过程涉及信息系统和用户之间的法律责任认定。用户每次交易时，需要对期货交易信息进行数字签名，用户的公钥证书为该信息系统自建的CA签发。在进行测评时，这种公钥证书的签发方式可能会导致“不可否认性”指标存在高危风险。	正确	错误		
4524	判断题	按照《信息系统密码应用高风险判定指引》，某二级信息系统在网络和通信安全层面，未使用密码技术实现通信前通信实体的身份鉴别，则密评时网络和通信安全层面身份鉴别测评单元的风险评价结果应为高风险。	正确	错误		
4525	判断题	依据《信息系统密码应用高风险判定指引》，某四级信息系统在网络和通信安全层面，存在安全接入认证需求，但采用密码技术实现短时间内难以实现，因此，可以通过设置白名单和终端ID绑定方式对该项测评指标面临的安全风险进行缓解。	正确	错误		
4526	判断题	依据《信息系统密码应用高风险判定指引》，新建二级信息系统如果未制定密码应用方案，密评时不会因未制定密码应用方案而面临高风险。	正确	错误		
4527	判断题	依据《信息系统密码应用高风险判定指引》，二级及以上的信息系统必须具备密码安全管理制度，否则在密评时会因不具备密码应用安全管理制度而面临高风险。	正确	错误		

4528	单项选择题	按照《商用密码应用安全性评估报告模板（2023版）》，如果信息系统密码应用方案的评估结果为通过，由此可得到该信息系统的密评结果为（）。	无法确定	符合	基本符合	通过
4529	单项选择题	按照《商用密码应用安全性评估报告模板（2023版）》，在编制系统密评报告时，以下不属于分析与报告编制活动内容的是（）。	单项测评结果判定	单元测评结果判定	风险分析	测评对象和测评内容确定
4530	单项选择题	国家密码管理局发布《关于规范商用密码应用安全性评估结果备案工作的通知》，进一步规范了商用密码应用安全性评估结果备案相关工作。通知中要求，各地区网络与信息系统运营者应当在密评报告出具之日起（ ）日内，填写《网络与信息系统密评备案信息表》，连同密评报告报密码管理部门备案。	10	30	60	90
4531	单项选择题	按照《商用密码应用安全性评估报告模板（2023版）》，方案密评报告和系统密评报告分别可以在（）阶段产生。	系统规划阶段和系统运行阶段	系统建设阶段和系统运行阶段	系统建设阶段和系统改造阶段	系统运维阶段和系统运行阶段
4532	多项选择题	按照《商用密码应用安全性评估报告模板（2023版）》，系统密评报告的封面应包含（）。	被测信息系统名称	合同编号	被测单位	密评机构
4533	单项选择题	按照《商用密码应用安全性评估报告模板（2023版）》，被测系统密评报告封面的报告编号应（）。	根据国家密码管理部门的编号要求进行编号	根据系统责任单位的文件归档要求进行编号	根据密评机构质量管理体系文件要求进行编号	根据信息系统网络安全等级保护备案编号进行编号
4534	单项选择题	按照《商用密码应用安全性评估报告模板（2023版）》中声明部分的相关内容，被测单位提供相关证据的（）对评估结论的有效性至关重要。	真实性	完整性	机密性	主动性
4535	单项选择题	根据《商用密码应用安全性评估报告模板（2023版）》，密评报告中给出的评估结论仅对被测信息系统（ ）的安全状态有效。	当年	当月	建成时	被测时

4536	单项选择题	根据《商用密码应用安全性评估报告模板（2023版）》，在（ ）的情况下，引用密评报告结论时可对其相关内容进行修改。	任何情况都不允许	系统发生变动	委托方授权	测评机构同意
4537	单项选择题	根据《商用密码应用安全性评估报告模板（2023版）》，三级信息系统的密评报告总体评价中，设备和计算安全层面测评结果可能存在（ ）。	符合2项，部分符合3项，不符合1项，不适用1项的情况	符合3项，部分符合2项，不符合2项，无不适用项的情况	符合2项，部分符合1项，不符合2项，不适用1项的情况	符合4项，部分符合2项，不符合1项，不适用1项
4538	单项选择题	根据《商用密码应用安全性评估报告模板（2023版）》，以下对信息系统密评报告“总体评价”章节描述错误的是（ ）。	总体评价章节中需要体现本次密评所依据GB/T 39786的级别要求	总体评价章节中需要体现本次密评的测评结果，包括测评项的符合情况及风险项数	总体评价章节中需要体现各个层面密码应用实施情况，但不需要体现测评项的符合情况	总体评价章节需要给出被测系统是否符合GB/T 39786相应等级指标要求的测评结论
4539	单项选择题	某三级信息系统通过调用密码模块为安全一级的服务器密码机（该密码机经检测认证合格），使用SM4算法(CBC模式）实现应用和数据安全层面重要业务数据存储机密性保护，则在信息系统密评报告“安全问题及改进建议”部分，以下选项中关于该测评结果面临的安全威胁分析合理的是（ ）。	设备资源被登录设备的非授权用户获取	搭建的远程管理通道被非授权使用，或传输的管理数据被非授权获取和篡改	密钥被非法获取，导致加密数据明文泄露	设备内重要程序和文件的来源不可信
4540	单项选择题	根据《商用密码应用安全性评估报告模板（2023版）》，（ ）应对密评报告的生命周期进行严格、规范的管理。	密评机构	密码管理部门	委托单位	被测单位
4541	单项选择题	某三级信息系统有两个机房，机房1的身份鉴别指标量化评估结果为0分，机房2的身份鉴别指标量化评估结果为0.5分，针对物理和安全层面的“身份鉴别”指标的量化评估和判定结果为（ ）。	0.25，部分符合	0，不符合	0.5，部分符合	无法判断

4542	单项选择题	某三级信息系统有两个机房A和B。其中，A机房的访问方式为“人工值守+视频监控”，访问人员经过审批后才可登记进入，该风险控制措施写入了该系统的密码应用方案中且方案通过了评估，密评人员到系统现场进一步核实了风险控制措施的使用条件和落实情况与方案描述相符。B机房有C和D两个门，无论从C门还是D门进入，都可以访问整个机房。C门的访问方式为（经检测认证合格的）电子门禁系统刷卡，D门的访问方式为ID卡。那么按照《商用密码应用安全性评估报告模板（2023版）》，该系统密评报告中，在物理和环境安全层面“身份鉴别”测评单元的判定结果为（）。	符合，1分	部分符合，0.5分	部分符合，0.75分	不符合，0分
4543	单项选择题	某三级信息系统有两个业务应用，应用1的用户A身份鉴别为符合，量化评估分值为1；用户B身份鉴别为部分符合，量化评估分值为0.5。应用2的用户身份鉴别为不符合，量化评估分值为0。按照《商用密码应用安全性评估报告模板（2023版）》，针对应用和数据安全层面的“身份鉴别”指标的量化评估和判定结果为（）。	0.5，不符合	0.75，部分符合	0.5，部分符合	0.75，不符合
4544	单项选择题	按照《商用密码应用安全性评估报告模板（2023版）》，某三级信息系统使用了自行设计（未经检测认证合格）且经过安全性证明的密码算法对业务系统重要数据进行保护，针对“应用和数据安全”层面的“重要数据存储机密性”指标最高可以给（）分。	0.25	0	0.5	1

4545	单项选择题	根据《商用密码应用安全性评估报告模板（2023版）》，管理制度中“具备密码应用安全管理制度”测评单元结果为部分符合，其量化评估分值可能为（ ）。	0	0.25	0.5	无法确定
4546	单项选择题	根据《商用密码应用安全性评估报告模板（2023版）》，在编制系统密评报告整体测评章节时，以下情况处理得当的是（ ）。	设备和计算安全层面中，堡垒机“系统资源访问控制信息完整性”和“日志记录完整性”保护采用通用操作系统自身安全机制实现，但如果堡垒机“身份鉴别”判定结果为“符合”，那么通过单元间的弥补后，前两项测评单元的判定结果可修正为“符合”	某省中心系统有与市中心系统业务交互需求，在应用和数据安全层面未采用密码技术对重要数据传输机密性保护。但采用了符合要求的密码技术对网络通信信道进行保护，且网络和通信安全层面测评指标的测评结果为符合。则“重要数据传输机密性”测评结果可修正为“符合”，弥补后分值为1分	某系统的设备远程管理路径为：管理员终端->SSL VPN网关->通用设备（静态口令登录）。所以只要终端到SSL VPN网关之间建立起基于国密SSL协议的网络通信通道，则通用设备“身份鉴别”测评单元可以由“不符合”弥补为“部分符合”，最高得0.5分	某第三方支付平台和银行有业务交互需求，在网络和通信安全层面未采用密码技术建立安全传输信道，通信报文的传输机密性无法得到保障。但在“应用和数据安全”层面，采用了符合要求的密码技术对重要数据传输机密性进行保护，且加密后的数据流能够覆盖网络通信信道。则“通信过程中重要数据的机密性”测评结果可以得到一定弥补
4547	单项选择题	根据《商用密码应用安全性评估报告模板（2023版）》，如果管理制度、人员管理、建设运行、应急处置四个方面的分数分别为1、1、0.5、0.5，则密码应用管理方面的总体得分为（ ）。	23	24	25	26

4548	单项选择题	根据《商用密码应用安全性评估报告模板（2023版）》，某三级信息系统，设备和计算安全层面应用服务器的“身份鉴别”指标为1分，应用和数据安全层面应用用户的“身份鉴别”指标为0分，则应用用户的身份鉴别经应用服务器的身份鉴别弥补后为（）。	1分	0.25分	0.5分	0分（无法弥补）
4549	单项选择题	根据《商用密码应用安全性评估报告模板（2023版）》，如果物理和环境、网络和通信、设备和计算、应用和数据四个层面的分数分别为1、1、0.5、0.5，则密码应用技术方面的总体得分为（）。	50	45	55	60

4550	单项选择题	根据《商用密码应用安全性评估报告模板（2023版）》，以下对信息系统密评报告“总体评价”及”测评结果记录”描述正确的是（ ）。	某二级信息系统责任单位编写有密码应用方案，且方案通过密评，在密码应用方案中对“系统资源访问控制信息完整性”测评项判定为不适用，但在实际测评过程中，系统责任单位对该测评项进行了密码保护，应依据密码应用方案，在“测评结果记录”中体现其不适用的情况	某信息系统通过未经认证的SSL VPN，使用HTTPS（V1.1）协议和AES-128-CBC算法，实现网络和通信安全层面业务数据传输通道通信过程中重要数据的机密性保护，在密评报告“测评结果记录”中D/A/K判定为√××	某信息系统在应用和数据安全层面，使用AES-128-CBC算法，实现重要业务数据存储的机密性保护。在密评报告“测评结果记录”中D/A/K判定为×/ /	某信息系统中部署了SSL VPN，该设备用于建立管理员从互联网登录VPN客户端接入内网的运维通道。管理员在内网，通过登录其专用的设备管理应用对该SSL VPN设备进行运维管理。那么在密评报告“测评结果记录”部分，描述其登录管理应用时的身份鉴别方式即可，无需描述管理员登录SSL VPN客户端的身份鉴别方式
4551	单项选择题	根据《商用密码应用安全性评估报告模板（2023版）》，在密评报告的测评结果修正部分，若测评对象A弥补了测评对象B的不足，测评对象A的分值为PA，测评对象B的弥补前分值为PB，则测评对象B弥补后的分值为（ ）。	PA	0.5×PA	MAX(0.5×PA, PB)	PB
4552	单项选择题	根据《商用密码应用安全性评估报告模板（2023版）》，风险等级不包括（ ）。	高	中	低	一般

4553	单项选择题	按照《商用密码应用安全性评估报告模板（2023版）》，系统密评报告中风险分析与（ ）完全无关。	不符合项或部分符合项导致的安全问题	关联威胁	资产价值	测评对象或测评单元分数
4554	单项选择题	按照《商用密码应用安全性评估报告模板（2023版）》，在编制系统密评报告时，某三级信息系统选取的基本指标数量为41，其中不适用指标4项，特殊指标0项，经整体测评后符合项20项，不符合项10项，部分符合项7项。那么风险分析结果中的高、中、低风险项数之和应为（ ）。	17	41	10	7
4555	单项选择题	按照《商用密码应用安全性评估报告模板（2023版）》，在编制系统密评报告风险分析部分时，以下描述正确的是（ ）。	如果系统中使用了SHA-1算法，那么该系统一定面临高等级安全风险	某个测评指标为不符合，量化评估分值为0分，经过风险分析后发现仅面临低等级安全风险，因此该指标的量化评估分数可以做相应的调整	如果某个安全层面的测评指标为不符合，该指标涉及测评对象测评对象B，其中测评对象A经分析后面临高等级安全风险，测评对象B经分析后面临中等级安全风险，那么该测评指标的最终风险等级应该为中	如果对测评结果中所有的不符合和部分符合项进行分析后发现存在高风险项，则认为信息系统面临高风险；同时也需要考虑多个中低风险叠加可能导致的高风险问题
4556	单项选择题	按照《商用密码应用安全性评估报告模板（2023版）》，信息系统商用密码应用安全性评估的评估结论能够判定为符合的情况是（ ）。	系统综合得分不低于60分	系统密码得分为100分	系统密码应用无中、高风险	系统综合得分不低于60分且系统密码应用无高风险

4557	单项选择题	密评人员在对某网络安全等级保护定级为第三级的OA办公系统的应急处置安全层面进行测评时发现，该系统责任单位制定并发布了详细的密码应用应急处置策略，在应急处置策略中明确了发生密码应用安全事件时的处置措施、报告流程以及完成事件处置后的汇报机制，设置了相应的责任岗位，相关应急处置策略合理可行，岗位职责明确，但现场测评发现，该系统从上线运行到本次密评，未发生过密码安全事件，且该系统未制定密码应用方案，则以下关于本系统“事件处置”和“向主管部门上报处置情况”两项指标的结果分析描述正确的是（ ）。	由于被测系统从上线运行至本次密评期间，均未发生密码安全事件，故事件处置、向主管部门上报处置情况均为不适用	由于被测系统从上线运行至本次密评期间，均未发生密码安全事件，仅有相应的应急管理制度，但无法验证其真在发生密码安全事件后能够按照相应的应急制度进行处置，故分别为不符合	由于被测系统从上线运行至本次密评期间，均未发生密码安全事件，仅有相应的应急管理制度，但无法验证其真在发生密码安全事件后能够按照相应的应急制度进行处置，故分别为部分符合	被测系统责任制定并发布了完善的密码应用应急处置策略，策略合理可行，人员岗位职责明确，故判定为符合
4558	单项选择题	按照《商用密码应用安全性评估报告模板（2023版）》，在对信息系统进行商用密码应用安全性评估时，需保证实施密评活动的人员中至少（ ）通过密评人员考试。	1名	2名	全员	无具体要求
4559	单项选择题	按照《商用密码应用安全性评估报告模板（2023版）》，以下属于信息系统密评报告“密评活动有效性证明记录”中“密评委托证明”中需要体现的内容的是（ ）	现场测评授权书	风险告知书	与密评机构签订的合同扫描件	差旅票证
4560	单项选择题	某面向公众的三级信息系统部署在政务云平台上，在对其开展密评工作时，由于外单位人员进入机房进行核查的审批流程繁琐，故密评机构与系统责任单位约定由系统责任单位运维人员代为前往机房进行设备核查，根据《商用密码应用安全性评估报告模板（2023版）》，这种方式是否符合密评要求（ ）。	符合	不符合	只要能够完成资产核查即可，进行核查的不一定为密评机构实施密评活动人员	目前没有相关要求

4561	单项选择题	按照《商用密码应用安全性评估报告模板（2023版）》，密评报告模板中报告声明页需（ ）。	加盖机构用章	加盖密评人员电子签章	机构法人签字	批准人签字
4562	多项选择题	按照《商用密码应用安全性评估报告模板（2023版）》，在编制系统密评报告时，针对云平台和云上应用的测评，以下表述合理的是（ ）。	如果云平台为SaaS服务模式，其上运行的电子签章系统仅用于支撑云上应用合同的抗抵赖保护，而不用于云平台本身，那么在对云平台测评时，需要对电子签章系统的支撑能力进行“部分评估”，并体现在系统密评报告中	如果云平台已经通过密评（即获得“符合”或“基本符合”的结论）且安全等级不低于云上应用，则目前针对云平台被完全评估的支撑能力，所对应的云上应用测评对象的测评结论可以为“不适用”	针对云平台被部分评估的支撑能力，可以在该云平台测评结论中体现相关支撑能力的名称、量化评估分值和适用条件、风险评估情况和适用条件	针对云平台被完全评估的支撑能力，可以在该云平台测评结论中体现相关支撑能力的安全层面、测评对象和所涉及的指标
4563	多项选择题	按照《商用密码应用安全性评估报告模板（2023版）》，以下有关云平台密评报告编写的描述错误的是（ ）。	云平台测评结论中应包含“云平台（密码）支撑能力说明”	在编写云平台密评报告时，被完全评估的支撑能力一般不涉及量化评估和风险判定过程	在编写云平台密评报告时，被部分评估的支撑能力一定不涉及量化评估和风险判定过程	云平台密评报告和传统信息系统密评报告所涉及的内容完全一致
4564	多项选择题	按照《商用密码应用安全性评估报告模板（2023版）》，以下有关云平台密评报告编写的描述正确的是（ ）。	云平台密评报告和传统信息系统密评报告所涉及内容不完全一致	云平台的密评报告中，应在云平台支撑能力分析环节对“被部分评估的支撑能力”的D/A/K分别进行判定	“云平台（密码）支撑能力说明”包含被完全评估的支撑能力、被部分评估的支撑能力两类	在编写云平台密评报告时，被完全评估的支撑能力一般不涉及量化评估和风险判定
4565	多项选择题	按照《商用密码应用安全性评估报告模板（2023版）》，信息系统密评报告中应包含（ ）。	单元测评结果	整体测评结果	风险分析	评估结论

4566	多项选择题	按照《商用密码应用安全性评估报告模板（2023版）》，信息系统密评报告中涉及编写测评对象的地方有（ ）。	测评对象确定结果	单元测评	测评结果记录	测评结果修正
4567	多项选择题	按照《商用密码应用安全性评估报告模板（2023版）》，下列关于密评结果备案的说法中，正确的内容包括（ ）。	密评结果备案的备案主体是信息系统运营者	所属北京市的信息系统的密评结果备案材料应首先提交到北京市密码管理部门	密评机构应每半年填写一次《密评机构工作情况统计表》并报送国家密码管理局	中央和国家机关有关部委规划建设的关键信息基础设施或者国家政务信息系统可以直接将密评结果备案材料报送国家密码管理局
4568	多项选择题	按照《商用密码应用安全性评估报告模板（2023版）》，密评报告不再适用的情况有（ ）。	被测信息系统业务发生重大变更	被评估密码应用方案发生变更	被测单位名称发生变更	委托双方合同期满
4569	多项选择题	按照《商用密码应用安全性评估报告模板（2023版）》，在任何情况下，若需引用密评报告中的评估结果或结论都应保持其原有的意义，不得对相关内容擅自进行（ ）。	增加	修改	伪造	掩盖事实
4570	多项选择题	按照《商用密码应用安全性评估报告模板（2023版）》，密评报告的被测信息系统基本信息表中，涉及到（ ）签字。	编制人	审核人	批准人	机构法人
4571	多项选择题	按照《商用密码应用安全性评估报告模板（2023版）》，以下应体现在信息系统密评报告“总体评价”章节中内容为（ ）。	不适用项数目	测评结果	风险项数目	系统密评得分
4572	多项选择题	按照《商用密码应用安全性评估报告模板（2023版）》，系统密评报告的评估结论包括（ ）。	符合	不符合	通过	不通过

4573	多项选择题	按照《商用密码应用安全性评估报告模板（2023版）》，以下关于信息系统密评报告中总体评价部分编制要求，描述正确的有（ ）。	总体评价为概要性描述，详细描述在报告第四章和结果记录部分已有详细描述，本章节仅需要给出各安全层面符合项、部分不符合项、不符合项、不适用项的数量统计结果即可，不需要展开说明	总体评价为概要性描述，除给出各安全层面符合项、部分不符合项、不符合项、不适用项的数量统计结果外，还需要对各安全层面密码应用的整体情况进行概要介绍	总体评价部分应说明测评中涉及的不适用项数量和具体的不适用项指标，不需要对不适用原因进行描述，不适用项不适用原因在结果记录和报告第四章均有具体描述	总体评价部分除对不适用项数量和具体的不适用项指标进行说明外，还需要对不适用的原因进行描述
4574	多项选择题	按照《商用密码应用安全性评估报告模板（2023版）》，以下关于信息系统密评报告的安全问题及改进建议部分编制要求，描述正确的有（ ）。	问题描述部分只需要将被测系统中主要问题列举出，无需逐一列出被测系统存在的密码应用安全问题	问题描述部分可根据报告“风险分析”章节中描述，按照各安全层面顺序，逐一列出被测系统存在的密码应用安全问题	改进建议要在符合密评要求的基础上，充分考虑其在被测系统中的可行性	改进建议提供通用的解决方案，能够满足密评要求即可，不用考虑其在被测系统中的可行性
4575	多项选择题	下列针对《商用密码应用安全性评估报告模板（2023版）》的说法中，正确的是（ ）。	被测信息系统基本信息表中，审核批准部分涉及编制人、审核人、批准人三类人员签字	三级信息系统，其密评报告的“总体评价”部分，设备和计算安全层面测评结果存在“符合2项，部分符合3项，不符合1项，不适用1项”的情况	密评结果记录应形成单独的文件，在密评结束后由密评机构归档，不用作为附件附在密评报告后面，密码管理部门需要检查时可要求密评机构提供	二级信息系统，其密评报告的“总体评价”部分，“管理制度”安全层面测评结果存在：符合1项，部分符合1项，不符合1项的情况
4576	多项选择题	按照《商用密码应用安全性评估报告模板（2023版）》，密评报告一般应在（ ）盖章。	封面和声明页	单元测评	报告附录	报告骑缝

4577	多项选择题	按照《商用密码应用安全性评估报告模板（2023版）》，密评报告中测评项目概述应包括（ ）。	测评目的	测评依据	测评过程	报告分发范围
4578	多项选择题	按照《商用密码应用安全性评估报告模板（2023版）》，以下（ ）文件应作为密评报告的依据。	GB/T 39786《信息安全技术 信息系统密码应用基本要求》	GM/T 0115《信息系统密码应用测评要求》	GM/T 0005《随机性检测规范》	《XXXXX系统密码应用方案》
4579	多项选择题	按照《商用密码应用安全性评估报告模板（2023版）》，密评报告中系统网络拓扑应说明（ ）。	系统体系架构	网络所在机房情况（物理机房的个数及其所在具体位置）	网络边界划分	与其他系统的互联关系（网络互联、数据互通等情况）
4580	多项选择题	按照《商用密码应用安全性评估报告模板（2023版）》，密评报告中现场测评方法通常包括（ ）。	访谈、文档审查	实地查看	配置检查	工具测试
4581	多项选择题	按照《商用密码应用安全性评估报告模板（2023版）》，现场测评方法中，访谈工作主要内容包括（ ）。	与被测单位的相关人员进行交流和问询	了解被测信息系统技术方面的基本信息	了解被测信息系统管理方面的基本信息	对测评内容进行确认
4582	多项选择题	按照《商用密码应用安全性评估报告模板（2023版）》，在文档审查中会涉及的文档有（ ）。	人员培训计划	安全管理制度文件	密钥管理制度	密码应用方案及评审意见
4583	多项选择题	按照《商用密码应用安全性评估报告模板（2023版）》，在编制系统密评报告单元测评部分时，需要注意（ ）。	单元测评中的测评对象需要与测评对象确定结果和测评结果记录（附录A）中的测评对象保持一致	单元测评结果分析中对于判定依据的相关描述需要与测评结果记录（附录A）中的保持一致	单元测评中的不适用指标应当与“测评范围与方法”中确定的不适用指标保持一致	单元测评结果中的测评指标符合情况需与整体测评结果中的符合情况保持一致（如果不存在测评结果修正）
4584	多项选择题	按照《商用密码应用安全性评估报告模板（2023版）》，系统密评报告的单元测评结果包括（ ）。	符合	不符合	部分符合	不适用

4585	多项选择题	按照《商用密码应用安全性评估报告模板（2023版）》，某三级信息系统只有一个网络通信信道，如果针对网络和通信安全层面的“身份鉴别”指标的判定结果为部分符合，其量化评估分值可能为（）。	0	0.25	0.5	无法确定
4586	多项选择题	按照《商用密码应用安全性评估报告模板（2023版）》，编制系统密评报告时，针对“网络和通信安全”层面的结果分析，以下描述不合理的是（）。	某三级信息系统，移动终端用户通过SSL VPN访问内网资源，移动终端与SSL VPN之间必须实现双向身份鉴别才能符合标准的要求	被测系统的远程管理通道存在跨网络的情况，跨网的信道不需要作为“网络和通信安全”层面的测评对象进行分析	某三级信息系统互联网PC端用户可以通过HTTP或者国密SSL协议两种方式访问被测信息系统，鉴于网络通信信道支持国密SSL协议，因此针对“通信过程中重要数据完整性”和“通信过程中重要数据机密性”指标可以判定为符合	某三级信息系统主机房和灾备机房之间通过部署IPSec VPN设备建立安全传输通道，测评人员将主机房到灾备机房和灾备机房到主机房的通信链路作为两个测评对象进行分析
4587	多项选择题	按照《商用密码应用安全性评估报告模板（2023版）》，对于应用和数据安全部分的报告编制，以下说法正确的是（）。	测评指标可分为“应用用户身份鉴别”、“重要数据安全”、“关键操作不可否认性”三类	应用用户可以是应用管理员和业务用户等	重要数据通常可分为“鉴别类”“业务类”“日志类”这三类数据	该安全层面的测评对象为应用系统，而不是应用用户、重要数据等
4588	多项选择题	按照《商用密码应用安全性评估报告模板（2023版）》，管理制度中“制定密码应用方案”测评单元结果为部分符合，其量化评估分值不可能为（）。	0	0.25	0.5	1

4589	多项选择题	按照《商用密码应用安全性评估报告模板（2023版）》，管理制度中“具备密码应用安全管理制度”测评单元结果为部分符合，其量化评估分值不可能为（）。	0	1	0.25	0.5
4590	多项选择题	按照《商用密码应用安全性评估报告模板（2023版）》，在编制系统密评报告时，以下与“建设运行”相关的测评对象包括（）。	密钥管理制度及策略类文档	应急处置记录	密评报告及密码实施方案	管理体系
4591	多项选择题	按照《商用密码应用安全性评估报告模板（2023版）》，系统密评报告中的测评结果修正是对（）开展的。	不适用指标	符合指标要求的测评对象	不符合指标要求的测评对象	部分符合指标要求的测评对象
4592	多项选择题	按照《商用密码应用安全性评估报告模板（2023版）》，在编制密评报告的整体测评部分时，需要注意的事项有（）。	测评对象作为整体测评时弥补的最小单位	弥补后的测评结果只能是“部分符合”	弥补后的分数最多0.5分	弥补后的分数最多0.25分
4593	多项选择题	按照《商用密码应用安全性评估报告模板（2023版）》，以下案例不能进行测评结果修正的是（）。	设备和计算安全层面的“身份鉴别”指标为符合，能够弥补设备和计算安全层面的“系统资源访问控制信息完整性”指标	应用和数据安全层面的“身份鉴别”指标为符合，能够弥补“重要数据存储机密性”指标	应用和数据安全层面“重要数据传输完整性”指标可以弥补网络和通信安全层面的“通信数据完整性”指标	堡垒机的身份鉴别判定结果为符合，可以弥补通用服务器的身份鉴别指标
4594	多项选择题	按照《商用密码应用安全性评估报告模板（2023版）》，以下应体现在信息系统密评报告“整体测评”章节中内容为（）。	总体评价	安全问题及改进建议	测评结果修正	整体测评结果和量化评估

4595	多项选择题	按照《商用密码应用安全性评估报告模板（2023版）》，编制系统密评报告时，以下说法不合理的是（ ）。	如果信息系统有密码应用方案且方案通过评估，针对密码应用方案中采用密码技术实现的指标，可以在系统密评报告的单元测评中直接判定为符合	如果安全管理方面的指标均不适用，那么被测系统的综合得分最高为70分	如果现场测评获取的技术证据与密码应用方案中描述的不一致，则应以密码应用方案中给出的技术措施为准	根据系统密评报告模板（2023版），测评结果修正只需要考虑层面间的弥补情况
4596	多项选择题	按照《商用密码应用安全性评估报告模板（2023版）》，系统密评报告中关于风险分析的体现，以下表述不合理的是（ ）。	如果被测系统确实涉及《信息系统密码应用高风险判定指引》中描述的高风险安全问题，那么测评结果记录中相关指标或测评对象的量化评估分值一定是0分	风险分析过程需要结合整体测评结果中的部分符合项或不符合项的关联威胁	如果系统涉及高风险判例中的问题场景，则需要在报告附录A中，按照实际评估结果进行填写，针对该测评项判定为不符合或部分符合，在风险分析时需要核查针对该安全风险是否存在缓解措施	被测系统的风险分析结果与被测系统的安全保护等级无关，即风险分析过程中不用考虑被测系统的安全保护等级

4597	多项选择题	按照《商用密码应用安全性评估报告模板（2023版）》，在编制系统密评报告风险分析环节时，以下情况处理合适的是（ ）。	某三级信息系统的设备仅支持本地运维，其登录方式为“用户名+口令+指纹”，这种情形下设备和计算安全层面的“身份鉴别”指标的风险等级可酌情降低	某第三方支付平台和银行有业务交互需求，在应用和数据安全层面未采用密码技术对重要数据进行传输机密性保护。但采用了符合要求的密码技术建立网络通信信道，且网络和通信安全层面适用指标的测评结果为满分。因此“重要数据传输机密性”的风险等级可酌情降低	某三级信息系统的设备远程管理路径为：管理员终端-SSL VPN网关-通用设备（静态口令登录）。通用设备只能通过SSL VPN网关访问登录（由访问控制策略保证），若SSL VPN网关登录方式符合密评要求，则通用设备“身份鉴别”的风险等级可酌情降低	某省中心系统和市中心系统有业务交互需求，在网络和通信安全层面未采用密码技术建立安全通信信道，通信报文的传输机密性无法得到保障。但采用了符合要求的密码技术对重要数据传输机密性进行保护，且加密后的数据流能够覆盖网络通信信道。因此“通信过程中重要数据的机密性”的风险等级可酌情降低
4598	多项选择题	按照《商用密码应用安全性评估报告模板（2023版）》，对系统密评报告中的风险分析表格描述错误的是（ ）。	风险分析时可从威胁类型和威胁发生频率等方面阐述	表格中每一行是一个测评对象的问题描述、关联威胁、风险分析和风险等级	在网络和通信安全层面关联的安全威胁包括“非法设备从外部接入内部网络，或网络边界被	在填写表格时，只需要注意识别出的高风险，无需考虑多个中低风险叠加而导致的高风险问
4599	多项选择题	按照《商用密码应用安全性评估报告模板（2023版）》，以下内容中应体现在系统密评报告中“商用密码应用安全性评估结论”的包括（ ）。	系统简介	测评情况简介	评估结论及综合得分	系统测评指标的符合情况及数目

4600	多项选择题	根据《商用密码应用安全性评估报告模板（2023版）》，分析以下给出的密评报告中“A.测评结果记录”示例，其中错误的是（　）	测评项：应用和数据安全层面身份鉴别 测评对象：金融IC卡 结果记录：某银行三级IC卡发卡系统，已完成国密改造并通过验收，该系统为用户分发了合规的金融IC卡（通过安全认证，密码模块等级为二级），用户在ATM机（或POS机上）插入IC卡进行联机交易时，在交易前首先通过在密码键盘输入PIN码实现对ATM（或POS）对金融IC卡的鉴别，未使用密码技术实现金融IC卡联机认证，因此该测评对象身份鉴别判定结果为不符合。 量化判定：错/错/错	测评项：应用和数据安全层面数据存储机密性 测评对象：用户支付口令 结果记录：某银行三级的网银系统，其系统注册用户的用户支付口令存储在数据库服务器中，数据库服务器通过调用合规的签名验签服务器（通过安全认证，密码模块安全等级为二级）使用SM4算法（CBC模式）实现了用户支付口令存储机密性保护。用户支付口令存储加密密钥由合规的签名验签服务器生成，仅用于用户支付口令存储机密性保护，该密钥加密存储在签名验签服务器中，不涉及分发、导入导出。因此该测评对象存储机密性判定结果为符合。 量化判定：对/对/对	测评项：设备和计算安全层面身份鉴别 测评对象：堡垒机 结果记录：受测系统管理员通过用户名+静态口令+动态口令登录堡垒机，通过在堡垒管理应用中集成动态令牌认证系统，并为用户配置动态令牌，使用合规的SM3算法实现用户的身份鉴别，身份鉴别涉及的密钥为动态令牌种子密钥，动态令牌种子密钥由服务器密码机产生，在堡垒机和动态令牌中存储、使用，不涉及分发、更新、备份、恢复、归档、撤销和销毁系统部署和使用的动态令牌为经检测认证合格的密码产品（密码模块等级为二级），因此该测评对象身份鉴别判定结果为符合。 量化判定：对/对/对	测评项：应用和数据安全层面身份鉴别 测评对象：应用用户 受测系统为App，应用用户通过用户名+口令+APP 扫码登录，APP集成了移动智能终端二级密码模块：通过身份认证网关、移动智能终端安全密码模块，使用合规的SM3WithSM2算法通过挑战响应机制实现身份鉴别。密钥管理由合规的密码产品执行，移动智能终端安全密码模块、身份认证网关，均具有商用密码产品认证证书，证书由合规的电子认证服务机构签发 量化判定：对/对/对

4601	多项选择题	按照《商用密码应用安全性评估报告模板（2023版）》，在信息系统密评报告中“密评活动有效性证明记录”部分，应体现的密评活动质量文件有（）。	现场测评授权书及风险告知书	测评方案的评审记录及确认记录	方案密评报告的评审记录及确认记录	系统密评报告的评审记录
4602	多项选择题	按照《商用密码应用安全性评估报告模板（2023版）》，在密评报告“密评活动有效性证明记录”中，在“密评委托证明”部分，需要提供证明文件（ ）才能满足密评报告形式审查要求。	合同关键页，需包含服务内容、收费金额、签字盖章等关键页	任务书关键页，需包含任务内容、任务委托单位、任务资金支持（如有）、签字盖章等关键页	其他委托证明文件，需包含委托内容、委托单位、签字盖章等关键页	运营者自行开展密评的，无须提供
4603	判断题	按照《商用密码应用安全性评估报告模板（2023版）》，即便信息系统密码应用方案通过了评估，那么针对某个安全层面的某个测评指标或者某个测评指标相关的测评对象，可能存在系统密评报告与方案密评报告中的判定结果不一致的情况。	正确	错误		
4604	判断题	某云平台为三级信息系统，已进行了密评，评估结论为基本符合。在该云平台上部署有一个四级信息系统（云上应用），在对该云上应用进行密评时，应依据云平台密评时的“云平台支撑能力说明”，采信“被完全评估的支撑能力”所对应测评对象的测评结果。	正确	错误		
4605	判断题	按照《商用密码应用安全性评估报告模板（2023版）》，委托密评机构开展密评的运营者，可以委托密评机构具体承担备案工作。	正确	错误		
4606	判断题	按照《商用密码应用安全性评估报告模板（2023版）》，被测信息系统业务发生重大变更后，应重新对其进行评估，已出具的密评报告不再适用。	正确	错误		

4607	判断题	按照《商用密码应用安全性评估报告模板（2023版）》，密评结论不能作为系统构成组件（如密码产品）的评估结论。	正确	错误		
4608	判断题	按照《商用密码应用安全性评估报告模板（2023版）》，二级系统的密评报告总体评价中，管理制度安全层面测评结果可能存在：符合1项，部分符合1项，不符合1项的情况。	正确	错误		
4609	判断题	按照《商用密码应用安全性评估报告模板（2023版）》，被测信息系统“总体评价”部分的部分符合项及不符合项数量总和，与“安全问题及改进建议”中的高、中风险数量总和应该一致。	正确	错误		
4610	判断题	应用和数据安全层面的密码应用通常与信息系统承载的业务息息相关，这部分应是密评报告中“密码应用情况”章节重点描述的内容。	正确	错误		
4611	判断题	根据《商用密码应用安全性评估报告模板（2023版）》，在密评报告中，应在“测评工具检查点”章节体现对系统中部署的每个设备的配置检查，且需要体现对信息系统传输、存储的数据进行抓取、分析。	正确	错误		
4612	判断题	根据《商用密码应用安全性评估报告模板（2023版）》，GB/T 39786《信息安全技术 信息系统密码应用基本要求》中不适用于被测信息系统的密码应用要求的个别项称为不适用指标。	正确	错误		

4613	判断题	根据《商用密码应用安全性评估报告模板（2023版）》，在信息系统密评报告中，如某一测评指标中的部分测评对象存在不适用情况，则应在报告“不适用指标”中体现，并说明该部分测评对象在该测评指标中的不适用原因。	正确	错误		
4614	判断题	根据《商用密码应用安全性评估报告模板（2023版）》，在密评报告中，测评工具检查点部分应描述在何处接入何种测评工具进行何种测试工作。	正确	错误		
4615	判断题	根据《商用密码应用安全性评估报告模板（2023版）》，单元测评中不同测评对象的结果判定应依据附录A测评结果记录中各个测评对象的量化评估分值来确定。	正确	错误		
4616	判断题	在编写系统密评报告（2023版）时，“单元测评”中的测评对象应该与“测评对象确定结果”中的测评对象保持一致。	正确	错误		
4617	判断题	在《商用密码应用安全性评估报告模板（2023版）》中，如果附录A测评结果记录中某个测评单元的测评对象量化评估结果为0.25分或0.5分，则在“单元测评”环节中该测评对象的结果应写部分符合。	正确	错误		
4618	判断题	《商用密码应用安全性评估报告模板（2023版）》中的单元测评结果为“弥补”修正后的结果。	正确	错误		
4619	判断题	根据《商用密码应用安全性评估报告模板（2023版）》，在编制系统密评报告时，对于网络和通信安全层面的测评结果可以仅依据访谈和实地查看提供的证据给出。	正确	错误		

4620	判断题	根据《商用密码应用安全性评估报告模板（2023版）》，如果被测系统存在弥补的情况，那么在完成测评结果修正后需要同步修改系统密评报告中第4章的单元测评结果。	正确	错误		
4621	判断题	在《商用密码应用安全性评估报告模板（2023版）》中，整体测评分为测评结果修正、整体测评结果和量化评估。其中测评结果修正要按测评单元、测评对象，填写弥补前和弥补后的测评结果和分值，并说明弥补原因。	正确	错误		
4622	判断题	根据《商用密码应用安全性评估报告模板（2023版）》，“测评结果修正”是针对“单元测评”中所有测评指标要求的测评对象进行分析是否存在弥补的情况。	正确	错误		
4623	判断题	根据《商用密码应用安全性评估报告模板（2023版）》，如果被测系统为三级信息系统，则整体测评结果汇总表中的“符合”“部分符合”“不符合”“不适用”指标项数之和应为41。	正确	错误		
4624	判断题	根据《商用密码应用安全性评估报告模板（2023版）》，编制系统密评报告时，如果安全管理四个层面均为不适用，那么该系统最高得分为70分。	正确	错误		
4625	判断题	根据《商用密码应用安全性评估报告模板（2023版）》，系统密评报告中的整体测评结果为修正后的整体测评结果和量化评估分数。	正确	错误		

4626	判断题	根据《商用密码应用安全性评估报告模板（2023版）》，在编制系统密评报告的风险分析内容时，如果不存在《商用密码应用安全性评估高风险判定指引》中的高风险项，则可以判定被测系统一定不会面临高风险。	正确	错误		
4627	判断题	密评人员在编制系统密评报告风险分析部分时，将网络和通信安全“通信过程中重要数据的机密性”测评单元降至中低风险，并给出如下分析：在网络和通信安全层面未采用密码技术建立安全通信信道，但采用了符合要求的密码技术对重要数据传输机密性进行保护，因此“通信过程中重要数据的机密性”的风险等级可以酌情降低。报告审核人员认为该风险缓解分析是到位的。	正确	错误		
4628	判断题	在《商用密码应用安全性评估报告模板（2023版）》中，可按照威胁类型和威胁发生频率进行风险分析，并将单元测评后的部分符合项或不符合项逐一进行关联威胁确认、风险分析和风险等级判定。	正确	错误		
4629	判断题	被测系统责任单位制定有密码应用应急处置方案，但截至目前系统未发生过密码应用相关安全事件，根据《商用密码应用安全性评估报告模板（2023版）》，应在信息系统密评报告的“检测结果记录”部分将“事件处置”、“向有关主管部门上报处置情况”两个测评项判定为“不适用”。	正确	错误		

4630	判断题	某三级信息系统在其通过密评的密码应用方案中将“不可否认性”作为不适用项，并说明系统无不可否认性保护需求，密评机构测评人员在实际测评过程中，发现该系统存在不可否认性应用场景，依据通过密评的密码应用方案，应在信息系统密评报告“检测结果记录”部分将该项判定为“不适用”。	正确	错误		
4631	判断题	根据《商用密码应用安全性评估报告模板（2023版）》，当被测信息系统经过测评结果修正，涉及到单元间或层面间的分值调整时，在信息系统密评报告的“检测结果记录”部分将测评对象及测评单元的原始分值替换为调整后的得分即可。	正确	错误		
4632	判断题	根据《商用密码应用安全性评估报告模板（2023版）》，当被测信息系统中存在可能涉及高风险的安全问题，但因为具备一定的缓解措施而降低为中风险时，应在信息系统密评报告测评结果记录部分修正测评结果为部分符合。	正确	错误		
4633	判断题	根据《商用密码应用安全性评估报告模板（2023版）》，密评结果记录应形成单独的文件，在密评结束后由密评机构归档，不用作为附件附在密评报告后面，密码管理部门需要检查时可要求密评机构提供。	正确	错误		

4634	判断题	某单位规划在2023年新建一个三级信息系统（协同办公信息系统），按照《国家政务信息化项目建设管理办法》（国办发[2019] 57号）要求，系统建设完成后应通过商用密码应用安全性评估。为简化招投标流程，A单位将密评事项在建设之初，就全权委托给系统建设总集成商单位B，由B单位选择相应密评机构，并B单位与密评机构签订测评委托协议，向密评机构支付密评费用，三方约定密评机构出具的最终密评报告仅交付给A，根据《商用密码应用安全性评估报告模板（2023版）》，这种情况符合密评管理要求。	正确	错误		
4635	单项选择题	如果基于数字证书方式进行用户的身份鉴别，在进行密评时，以下核查（ ）不是必要的。	检查根证书如何安全导入或预置到系统内	检查数字证书的合规性	验证数字证书的证书链是否通过	检查数字证书的机密性是如何保证的
4636	单项选择题	以下选项（ ）不是对传输完整性实现的测评方法。	利用Wireshark分析受完整性保护的数据在传输时的数据格式（如签名长度、MAC 长度）是否符合预期	如果采用数字签名技术进行传输完整性保护，测评人员可以使用公钥对抓取的签名结果进行验证	条件允许的情况下，测评人员可尝试对传输数据进行篡改（如修改MAC 值 或数字签名值），验证完整性保护措施的有效性	检查传输过程是否符合GB/T 15843《信息技术 安全技术 实体鉴别》要求
4637	单项选择题	以下选项（ ）不被认为是云平台“完全评估的支撑能力”。	仅为租户应用提供的电子签章服务	云平台所在的物理机房环境	云平台管理应用	云平台提供的设备运维通信信道
4638	单项选择题	Linux系统的用户口令一般存储在路径（ ）下。	/etc/group	/etc/shadow	/etc/login.defs	/etc/named.conf

4639	单项选择题	Linux系统的用户口令一般存储在/etc/shadow路径下，口令存储字符串格式为：idsalt$encrypted，其中id为1时表示口令采用（）密码算法进行杂凑后存储。	MD5	Blowfish	SHA-256	SHA-512
4640	单项选择题	在测评过程中遇到的PEM编码格式，除了开头和结尾，其内容体通常以（）格式编码。	BER	DER	Base64	Base64url
4641	单项选择题	某信息系统部署在云服务提供商（CSP）机房，其物理机房完全由CSP托管，那么在对该信息系统进行密评时，在物理和环境安全层面合理的做法是（）。	若CSP机房未通过密评，则物理和环境安全层面直接判定为“不符合”	若CSP机房通过密评，则可以复用该机房的密评结论	若CSP机房未通过密评，则可以直接判定为“符合”	无论CSP机房是否通过密评，物理和环境安全层面应判定为“不适用”
4642	单项选择题	某二级信息系统，对物理和环境安全层面“身份鉴别”这一项，其密码应用方案中论述了无法采用密码技术的客观因素，并提供了目前采用的风险控制措施，即人脸识别，密评人员在实际测评时核实密码应用方案中的措施已落实。那么作为该条款的测评结论合理的是（）。	符合	部分符合	不符合	不适用
4643	单项选择题	在设备和计算安全层面，若存在100台服务器，其中60台为A厂商生产且为同一型号，40台为B厂商生产且为同一型号，同一厂商的硬件/软件配置相同。为提高测评效率，同时避免遗漏测评对象，以下测评对象选取方法合理的是（）。	同一类机型的服务器作为一个测评对象，所以有两个测评对象，即机型A和机型B两类服务器	由于这100台服务器均属于通用设备，可视为一个测评对象	每一台服务器均作为一个测评对象，所以测评对象数量为100个	以上都正确
4644	单项选择题	某四级信息系统，对物理和环境安全“身份鉴别”这一项，其密码应用方案中论述了无法采用密码技术的客观因素，并提供了目前采用的风险控制措施，即“口令+指纹”，密评人员在实际测评时核实方案中的措施已落实。那么作为该条款的测评结论合理的是（）。	符合	部分符合	不符合	不适用

4645	单项选择题	某三级信息系统开发人员采用密码机（经检测认证的一级密码模块）实现的SM4算法，为具有“重要数据传输机密性”安全需求的数据提供相应密码保护，经密评人员确认该指标测评对象有2个，且密码保护有效。那么该指标的判定结果较为合理的是（ ）。	符合，1分	部分符合，0.5分	部分符合，0.3分	不符合，0.25分
4646	单项选择题	用户在某银行网点取钱，输入支付口令后，该口令途经两段传输过程：1）ATM机到银行服务端金融数据密码机（经检测认证合格），采用SM4算法提供传输机密性；2）银行服务端金融数据密码机（经检测认证合格）到银行服务端核心系统服务器（非直连），采用AES-128提供传输机密性。以口令作为测评对象，其“重要数据传输机密性”的判定结果为（ ）。	符合	部分符合	不符合	基本符合
4647	单项选择题	以下因素（ ）可能导致数字签名功能不正确。	签名中使用固定的随机数	待签消息比SM3杂凑值长	签名中使用不可预测的随机数	使用私钥签名
4648	单项选择题	某信息系统在数据库中存储有用户的性别字段的密文，应用开发人员告知密评人员该字段采用SM4-CBC算法进行了加密。密评人员查看该字段信息发现只存在两种密文值，每个密文值长度为128比特。那么以下推断正确的是（ ）。	如果确实使用SM4-CBC进行加密，那么开发人员可能错误地使用了IV	由于密文长度为64比特的整数倍，因此性别字段一定使用了DES或3DES进行加密，开发人员说法存在问题	开发人员不可能使用ECB模式加密	由于密文长度为128比特的整数倍，符合SM4的分组特征，因此可以判定开发人员的说法是正确的

4649	单项选择题	应用服务器的数据库中，用户的单条记录（包括口令杂凑值、身份证号、手机号等密文值、角色、权限等）利用HMAC-SM3计算后，把得到的MAC值一并存放在该条目中，针对“应用和数据安全”层面的“重要数据存储完整性”指标判定最多可以给（ ）分。	0	0.25	0.5	1
4650	单项选择题	某三级信息系统所在机房部署符合GM/T 0036《采用非接触卡的门禁系统密码应用指南》的电子门禁系统，使用SM4算法进行密钥分散，实现门禁卡的“一卡一密”，并基于SM4算法对人员身份进行鉴别，因此该系统在“物理和环境安全”层面的“身份鉴别”指标的量化评估结果最多为（ ）分。	0.25	0.5	0	1
4651	单项选择题	某三级信息系统，网络和通信安全层面采用了合规的密码技术进行通信实体身份鉴别，测评人员经核实后判定结果为1分；应用和数据安全层面采用“用户名+口令”的方式对业务系统登录用户进行身份鉴别。则“应用和数据安全”层面的“身份鉴别”指标的应用用户测评对象经“网络和通信安全”层面“身份鉴别”指标结果弥补后的量化评估分值为（ ）。	1	0.5	0.25	0
4652	单项选择题	某三级信息系统通过HMAC-SM3对重要数据计算MAC值后与数据原文一同存储在数据库中，密码运算为软件实现，针对“应用和数据安全”层面的“重要数据存储完整性”指标最高可以给（ ）分。	0	0.25	0.5	1

4653	单项选择题	某三级信息系统的重要数据包括用户口令、日志信息、业务数据，这三类数据的存储机密性量化评估分值分别为0.25、0.5、0.25，针对“应用和数据安全”层面的“重要数据存储机密性”的测评单元得分为（ ）。	0.3333	1	0.5	0.25
4654	单项选择题	某三级信息系统，制定了密码安全应急策略，规定了相关应急事件处置措施和流程，明确了密码应用应急事件处置完成后及时向当地密码管理部门报告事件发生和处置情况。该系统目前未发生过密码应用安全事件，无相应处置记录。针对“应急处置”层面的“事件处置”指标最高可以给（ ）分。	1	0.25	0.5	0
4655	单项选择题	某三级信息系统的系统管理员通过堡垒机登录通用服务器并对其进行远程管理，进入堡垒机后，系统管理员通过用户名+口令的方式访问通用服务器。系统管理员登录堡垒机时通过部署具有商用密码产品认证证书的安全浏览器（安全等级二级）和智能密码钥匙（安全等级二级）并基于数字证书（在有效期内）的方式进行身份鉴别，算法为SM2。因此该系统在“设备和计算安全”层面的通用服务器测评对象的“身份鉴别”指标D、K的判定结果为（ ）。	√，√，√	×，/，/	√，×，×	√，√，×
4656	单项选择题	某三级信息系统用户端与服务端之间进行通信时，只对服务端进行了基于密码的身份鉴别且身份鉴别机制有效，使用的签名算法为SM2withSM3，针对“网络和通信安全”层面的“身份鉴别”指标最高可以给（ ）分。	0	0.25	0.5	1

4657	单项选择题	某三级信息系统通过堡垒机对通用服务器进行集中管理，其中管理员与堡垒机之间使用HTTP协议建立传输通道，堡垒机与通用服务器之间使用SSH2.0建立传输通道，因此针对“设备和计算安全”层面的“远程管理通道安全”指标的判定结果为（）。	符合	部分符合	不符合	无法判断
4658	单项选择题	某信息系统有两个业务应用，其中应用A有管理员用户和操作员用户两类用户，分别采用用户名+口令和基于动态口令（经过检测认证的密码产品）的身份鉴别方式；应用B有管理员用户和业务员用户两类用户，均基于经过检测认证的智能密码钥匙进行身份鉴别。针对“应用和数据安全”层面的“身份鉴别”指标，最多可以给（）分。	0.5	1	3	0.75
4659	单项选择题	某三级信息系统通过SSL VPN建立远程管理传输通道，管理终端与SSL VPN之间传输协议使用的密码套件为ECC_SM4_GCM_SM3。该网络通信信道使用（）算法实现通信数据的机密性保护。	ECC	SM4_GCM	SM3	基于SM3的HMAC
4660	单项选择题	某三级信息系统客户端与服务端之间的网络通信信道使用TLSv1.2协议进行传输保护，使用的密码套件为TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384，记录层协议中使用（）算法进行通信数据机密性和完整性保护。	ECDHE，RSA	AES_256_GCM,AES_256_GCM	AES-GCM，HMAC-SHA384	AES-GCM，SHA384

4661	单项选择题	某三级信息系统的访问控制信息通过调用服务器密码机（通过商用密码产品检测认证）使用SM3withSM2数字签名算法计算签名值后，将访问控制信息与签名值一同保存在数据库中，但用户访问业务应用时未对访问控制信息的签名值进行验证，针对“应用和数据安全”层面的“访问控制信息完整性”为（ ）分。	0	0.25	0.5	1
4662	单项选择题	在密评时，以下密码算法/技术的组合（ ）认为存在高危风险。	对数据进行RSA-3072和SHA-1签名	对数据进行DES加密后，再进行SM4加密	对数据进行HMAC-SHA256保护	对数据进行SM2和SM3签名
4663	单项选择题	测评过程中，对信息系统网络边界内的用户与系统应用之间重要数据传输保护的测评属于（ ）安全层面的测评内容。	网络和通信安全	设备和计算安全	应用和数据安全	密钥管理
4664	单项选择题	密评人员对SSL VPN进行测评时发现所使用的密码套件为{0xe0，0x11}，以下判断不合理的是（ ）。	该套件使用SM2密钥交换算法进行密钥协商	该套件使用SM4-GCM进行数据加密	该套件使用HMAC-SM3进行数据完整性保护	该套件使用SM2算法进行密钥协商
4665	单项选择题	密评人员对SSL VPN进行测评时发现所使用的密码套件为{0xe0，0x13}后，以下判断不合理的是（ ）。	该套件使用SM2密钥交换算法进行密钥协商	该套件使用SM4-CBC进行数据加密	该套件使用HMAC-SM3进行数据完整性保护	该套件使用SM3作为PRF派生密钥
4666	单项选择题	某业务系统用户手机号利用SM3进行杂凑计算后，将得到完整的杂凑值存放在应用服务器的数据库中，那么对于“应用和数据安全”层面的“重要数据存储完整性”指标最多可以给（ ）分。	0	0.25	0.5	1
4667	多项选择题	在测评时，信息系统声称采用SM4-CBC进行个人隐私信息的存储机密性保护，以下收集的证据与其声称的存在矛盾或证明其使用不合规的包括（ ）。	密文长度为192比特	密文长度为64比特	IV值以明文形式存储	IV值都为全0

4668	多项选择题	在密评中，当证书认证系统作为测评对象时，以下测评实施合理的包括（ ）。	对信息系统内部署证书认证系统，测评人员可以参考GM/T 0037《证书认证系统检测规范》和GM/T 0038《证书认证密钥管理系统检测规范》的要求进行测评	通过查看数字证书扩展项KeyUsage 字段，确定证书类型（签名证书或加密证书）， 并验证数字证书及其相关私钥是否正确使用	通过数字证书格式合规性分析，验证生成或使用的证书格式是否符合GM/T 0015《基于SM2 密码算法的数字证书格式规范》的有关要求	检查证书认证系统中所使用的密码机等是否具备商用密码产品认证证书
4669	多项选择题	在密评中，当电子门禁系统作为测评对象时，以下测评实施合理的包括（ ）。	尝试发一些错误的门禁卡，验证这些卡无法打开门禁	利用发卡系统分发不同权限的卡，验证非授权的卡无法打开门禁	对电子门禁系统是否满足GM/T 0028《密码模块安全技术要求》进行检测	检查电子门禁系统中所使用的智能卡、密码机等是否具备商用密码产品认证证书
4670	多项选择题	在密评中，当IPSec VPN保护的通道作为测评对象时，以下测评实施合理的包括（ ）。	抓取IPSec通信报文进行分析算法使用情况，以及对数字证书开展合规性分析	查看IPSec VPN的配置情况	检查IPSec VPN等是否具备商用密码产品认证证书	对IPSec VPN是否满足GM/T 0028《密码模块安全技术要求》进行检测认证
4671	多项选择题	如果设备登录需要使用智能密码钥匙，那么开展密评时，以下测评实施合理的包括（ ）。	在模拟的主机或抽选的主机上安装监控软件（如Bus Hound），用于对智能密码钥匙的APDU指令进行抓取和分析，确认调用指令格式和内容符合预期（如口令和密钥是加密传输的）	如果智能密码钥匙存储有数字证书，测评人员可以将数字证书导出后，对数字证书合规性进行检测	检查智能密码钥匙是否具备商用密码产品认证证书	对智能密码钥匙是否满足GM/T 0028《密码模块安全技术要求》进行检测认证

4672	多项选择题	在密评中发现被测信息系统使用了以下密码算法和密码技术，合规的是（ ）。	SM4-GCM	SM3-HMAC	TLS 1.3	TLCP
4673	多项选择题	在对信息系统进行密钥管理测评时，以下存在风险的有（ ）。	DH密钥协商前或协商过程中未进行身份鉴别	利用口令派生的密钥进行传输通信保护	一个密钥同时用于加密和MAC	IV和计数器值公开传递
4674	多项选择题	测评人员在测评时，发现以下情况，其中密码应用合规正确的有( )。	通信双方进行加密通信前，使用了双证书中的加密证书进行SM2密钥协商	通信双方使用TLS 1.3进行通信，并将其中的密码算法全部替换为SM2/SM3/SM4	用户使用SM4-CTR进行加密时，以随机数和当前时间值的拼接作为计数器值，将计数器值以明文形式与密文一并发送给接收方	信息系统使用同一个数据密钥采用SM4-CBC模式对所有用户的性别信息进行加密保护，并使用全0的IV值
4675	多项选择题	密评人员对SSL VPN进行测评时发现{0xe0，0x13}后，以下判断合理的是（ ）。	SSL VPN的两端进行了双向身份鉴别	SSL VPN的两端利用ECDH协议进行密钥交换	SSL VPN的两端采用SM4算法实现数据传输的机密性保护	SSL VPN的两端采用HMAC-SM3算法实现数据传输的完整性保护
4676	多项选择题	密评人员在检查数据库中存储的口令杂凑值时，发现以下情况：（1）A和B有相同的口令杂凑值；（2）口令杂凑值长度均为256比特。以下分析正确的是（ ）。	可以确定使用了SM3对口令进行杂凑保护	可能采用了MD5对口令进行杂凑计算	计算口令杂凑值时可能未加入用户唯一的盐值	A和B可能共享相同的口令
4677	多项选择题	对于托管到IDC机房的信息系统，测评其物理和环境安全层面，较为合理的做法有（ ）。	若IDC机房通过密评，则可以复用该机房的密评结论	若IDC机房未通过密评，对于条件不允许的情况，可通过IDC机房运维方提供的相关说明文件和有关证据，进而给出测评结论	若IDC机房未通过密评，则需要现场测评取证，判定该机房的符合程度	无论IDC机房是否通过密评，由于机房的责任主体不属于该信息系统责任方，所以该机房的测评结论应是“不适用”

4678	多项选择题	在测评某一信息系统时，其设备和计算安全层面可能涉及的测评对象有（ ）。	数据库管理系统	虚拟机	应用服务器	VPN网关
4679	多项选择题	重要数据存储完整性可以通过以下（ ）密码技术实现。	带盐的SM3	HMAC-SHA256	CMAC-SM4	SM2数字签名
4680	多项选择题	网络和通信安全层面的测评对象识别与确认应考虑以下因素（ ）。	网络类型	通信人员	传输数据	通信主体
4681	多项选择题	测评人员在核查“传输机密性”密码功能时，可能需要关注以下内容（ ）。	重要数据或鉴别信息是否为密文	密文数据长度是否符合预期	相关密码产品中密钥类型	相关密码产品中密码算法类型
4682	多项选择题	测评人员在核查“传输完整性”密码功能时，可能需要关注以下内容（ ）。	数字签名数据长度	MAC值长度	使用对应公钥能否对签名值通过验签操作	相关密码产品中加密算法类型
4683	多项选择题	测评人员在核查“真实性”密码功能时，可能需要关注以下内容（ ）。	发送的挑战值是否每次均不重复	使用对应公钥能否对签名值通过验签操作	公钥或对称密钥与实体的绑定方式	对数字证书格式正确性进行验证
4684	多项选择题	对某政务外网信息系统开展测评时，网络和通信安全层面的测评对象可包括（ ）。	互联网用户通过浏览器访问该系统服务网站的HTTP通信信道	该系统与政务外网上其他单位的系统之间的通信信道	异地办事人员访问该系统建立的VPN通信信道	该系统移动端APP访问服务端建立的HTTPS通信信道
4685	多项选择题	以下关于用户密钥的存储方式，说法正确的是（ ）。	数据加密密钥在经过检测认证的三级密码模块中存储	SM2签名私钥经SM4-GCM加密后存储在数据库中	SM2签名证书明文存储在应用服务器中	SM4密钥经SHA1加密存储在数据库
4686	多项选择题	应急广播消息一般用于发布事关人民群众的生命财产安全的内容，消息发布过程一旦遭到非授权破坏，将会严重扰乱社会秩序。针对应急广播业务场景中应急广播消息的安全需求分析，正确的是（ ）。	消息来源真实性	消息传输机密性	消息播发行为的不可否认性	消息传输完整性
4687	多项选择题	在电子不停车收费系统（ETC）中，车辆通过办理和安装ETC卡，实现车辆在高速收费站的流水数据的产生、传输和缴费等功能。对于该业务场景的安全需求分析，正确的是（ ）。	车辆途经收费站时，收费站和车辆的双向鉴别	车辆信息、扣费金额等业务数据的传输完整性	收费站将ETC业务数据传输到省联网收费中心时的网络通信实体身份鉴别	收费站将ETC业务数据传输到省联网收费中心时的通信数据完整性保护

4688	多项选择题	关于电子门禁系统的实操测试，以下描述正确的有（ ）。	尝试复制门禁卡，验证是否可以进行有效复制	修改某一条门禁访问日志记录，验证是否有篡改成功	对每条记录分别生成MAC值并存放在该条记录后面一列的做法是可以满足“电子门禁记录数据存储完整性”要求的	利用发卡系统分发不同权限的卡，验证未授权的卡无法打开门禁
4689	多项选择题	信息系统中使用的服务器密码机作为测评对象，针对“设备和计算安全”层面的“身份鉴别”指标，服务器密码机采用以下（ ）鉴别方式时可以判定为符合。	智能IC卡	智能密码钥匙+口令	口令	智能密码钥匙
4690	多项选择题	针对“应用和数据安全”层面的“身份鉴别”指标，以下登录方式最高可以得1分的是（ ）。	用户名+短信验证码	用户名+智能密码钥匙+PIN码	人脸+指纹	用户名+动态令牌
4691	多项选择题	某三级信息系统已运行5年，针对“建设运行”部分的“定期开展密码应用安全性评估及攻防对抗演习”指标开展测评时，以下（ ）可以作为测评证据。	上一次的密评报告	攻防对抗演习报告	对上一次密评过程中存在的问题进行整改的文件	等级保护测评报告
4692	多项选择题	信息系统中使用的用于业务数据保护的密钥，以下做法不正确的是（ ）。	同一个密钥既用于加密保护又用于安全认证	公钥明文存储在数据库中，未进行完整性保护	在进行签名验签前未对公钥证书有效性进行验证	对签名私钥进行归档
4693	多项选择题	某网上银行交易系统，用户交易信息由用户智能密码钥匙使用SM2算法进行数字签名后传输，实现交易数据原发行为的不可否认性，数字签名算法实现正确。针对“应用和数据安全”层面的“不可否认性”指标，可能的分值是（ ）。	0	0.25	0.5	1

4694	多项选择题	以下情况可能会导致系统的整体评估结论为“不符合”的是（ ）。	某三级信息系统制定了密码应用方案且方案通过评审，在测评时发现系统存在一个高风险项	在对某运行过程中的四级信息系统进行测评时发现，被测单位未建立任何与密码应用安全管理活动相关的管理制度	某三级信息系统未采用密码技术对存储的重要数据进行完整性保护，但系统具有符合要求的身份鉴别措施，保证只有授权人员才能访问应用系统的重要数据，且定期对重要数据进行备份	某四级电子公文系统使用RSA-1024、SHA-1算法对业务员的关键行为进行数字签名，以实现关键操作行为的不可否认性
4695	多项选择题	在对医疗机构信息系统进行测评时，涉及不可否认性需求的可能有（ ）。	病例完成时间的不可否认性	医护人员开具处方的不可否人性	患者知情同意文书签署的不可否认性	电子病例书写的不可否任性
4696	多项选择题	某四级信息系统的责任单位可采用以下（ ）机制以满足“人员管理”方面的要求。	设置密钥管理员、密码安全审计员、密码操作员并分别由甲、乙、丙三人担任	关键岗位人员由机构内部人员担任，并在任前进行背景调查	建立上岗人员培训制度，对涉及密码的操作和管理人员进行专门培训	建立人员保密和调离制度，签订保密合同
4697	多项选择题	云平台中使用的云服务器密码机作为测评对象时，应满足以下管理要求（ ）。	云服务器密码机的宿主机由云平台或云服务器密码机所有者进行管理和使用，虚拟密码机由租户管理和使用	宿主机和不同的虚拟密码机不能相互访问对方的管理员账号、口令	云服务器密码机的宿主机接受云平台管理系统的集中统一管理，虚拟密码机不接受云平台管理系统的集中统一管理，可由虚拟密码机所属租户自己的管理系统进行集中统一管理	云服务器密码机的宿主机和不同虚拟密码机的远程管理通道应彼此独立，并采用加密和身份鉴别等技术手段对远程管理通道进行保护

4698	多项选择题	针对“网络和通信安全”层面的测评，以下描述不合理的是（ ）。	某三级信息系统，移动终端用户通过SSL VPN访问内网资源，移动终端与SSL VPN之间必须实现双向身份鉴别	如果被测系统的远程管理通道存在跨网络的情况，那么该远程管理通道也应该作为“网络和通信安全”层面的测评对象	某三级信息系统互联网PC端用户可以通过HTTP或者国密SSL协议两种方式访问被测信息系统，针对“通信数据完整性”和“通信过程中重要数据机密性”指标可以直接判定为符合	某三级信息系统主机房和灾备机房之间通过部署IPSec VPN设备建立安全传输通道，那么该网络通信信道的测评只能以主机房的IPSec VPN设备作为测评接入点
4699	多项选择题	在车路协同通信场景中，可以采用以下（ ）方式开展测评。	在被测车辆无线通信范围内，使用无线协议分析类工具抓取智能车辆发送的通信数据，核实其消息中是否附加了数字签名	通过文档审查、配置检查等方式验证车辆接收消息时是否验证了数字签名以及签名所用证书的有效性	在核实数字证书合法性和有效性时，应注意数字证书管理的各个环节	查看和核实信息系统使用的各密码产品的商用密码产品认证证书
4700	多项选择题	如果发现被测信息系统采用对称密码体制，使用“密钥加密密钥-数据密钥”的二层密钥体系进行数据的传输加密，以下测评实施合理的包括（ ）。	检查密钥加密密钥分发时是否抗截取、篡改、假冒等攻击	检查密钥加密密钥分发时密钥的机密性、完整性等	检查数据密钥分发时是否抗截取、篡改、假冒等攻击	检查数据密钥分发时密钥的机密性、完整性等
4701	多项选择题	某四级信息系统中，采用SSL VPN保护通信信道，使用Wireshark工具得知所使用的套件为ECC_SM4_SM3，但没有抓取到Certificate Request报文，以下分析正确的是（ ）。	该通道可以满足双向鉴别的“身份鉴别”指标要求	该通道无法满足双向鉴别的“身份鉴别”指标要求	在Server Certificate报文可以抓取到SM2证书	抓包时无法获得客户端证书

4702	多项选择题	关于数字证书的使用，以下存在风险的有（ ）。	证书中未标明持有者的身份	证书在使用前未验证真实性和有效性	未及时更新CRL或未使用OCSP查询证书状态	CA签发的用户证书在未保护的通道中进行分发
4703	多项选择题	某信息系统采用专线来进行网络传输，但未采用密码技术进行保护。以该专线作为测评对象时，以下说法正确的是()。	量化评估时，该测评对象的分值为0.5	量化评估时，该测评对象的分值为0	该测评对象的测评结果可能会导致信息系统整体测评结果为“不符合”	该测评对象的测评结果将一定不会导致信息系统整体测评结果为“不符合”
4704	多项选择题	以下做法正确的有（ ）。	利用经检测认证合格的智能密码钥匙、智能 IC 卡、动态令牌等作为用户登录应用的凭证	使用SM2对口令加密后传输，实现可抗重放攻击的身份鉴别	利用经检测认证合格的服务器密码机等设备对重要数据进行加密、计算 MAC 或签名后存储在数据库中，实现对重要数据在存储过程中的保密性和完整性保护	利用经检测认证合格的签名验签服务器、智能密码钥匙、电子签章系统、时间戳服务器等设备实现对可能涉及法律责任认定的数据原发、接收行为的不可否认性保护
4705	多项选择题	某信息系统客户端APP与服务端之间通过SSL VPN建立的安全传输通道，对网络和通信安全进行保护，通过抓取和分析通信数据包，使用的密码套件为TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384，以下分析正确的是（ ）。	该协议使用RSA密码算法的数字信封功能进行密钥协商	该协议使用AES-256的GCM工作模式保护传输数据的机密性	无法确定所使用RSA算法的密钥长度，还需要抓取传输中涉及的证书进行判断	该协议使用AES-256的GCM工作模式保护传输数据的完整性
4706	多项选择题	经检测认证合格的密码产品作为测评对象，关于其设备和计算安全层面的判定，正确的是（ ）。	身份鉴别一定是“符合”	日志记录完整性为“符合”	远程管理通道安全性一定是“不适用”	重要可执行程序完整性、重要可执行程序来源真实性为“符合”
4707	多项选择题	针对车联网OTA升级场景下的安全需求分析，正确的是（ ）。	智能网联汽车接入运营商网络的安全认证	OTA平台与智能网联汽车的通信实体真实性	OTA升级包来源的真实性	OTA升级包传输完整性

4708	多项选择题	在针对“设备和计算安全”层面进行测评时，以下描述较为合理的是（ ）。	交换机、网闸、防火墙一般不作为设备和计算安全层面的测评对象	某三级信息系统部署了3台同一型号的SSL VPN，在密评报告中可以将这三个SSL VPN作为一个测评对象，但在进行量化评估时，D/A/K需以这三个SSL VPN的实际应用情况的最低分值赋分	设备和计算安全层面的“身份鉴别”指标无法弥补“应用和数据安全”层面的“身份鉴别”指标	针对整机类密码产品的“身份鉴别”指标可以直接判定为符合
4709	判断题	对各个层面的“身份鉴别”指标测试时，主要检查所使用的密码算法是否合规和相应的密钥管理是否安全，抗重放攻击不是该指标的考察范围。	正确	错误		
4710	判断题	如果某个服务器密码机部署在核心交换机上，且没有部署必要的逻辑隔离措施，这种部署方式存在很高的安全隐患。	正确	错误		
4711	判断题	在进行测评时，发现某系统的主密钥采用知识拆分的方式进行导出，但是在做密钥分片存储时，使用同一个人的同一个智能密码钥匙进行保存，这种方式是不安全的。	正确	错误		
4712	判断题	判断以下做法是否正确：CA签发证书后，用户将私钥和数字证书存放在用户的U盘内保存。	正确	错误		
4713	判断题	公钥必须保护其与实体的绑定关系，对称密钥没有这种必要，因此在测评时，主要关注的是对称密钥的机密性和完整性。	正确	错误		

4714	判断题	因通信链路上可能承载多个不同应用，这些应用可能需要对各自的用户实施更细粒度的身份标记和鉴别，因此，网络和通信安全层面的鉴别一般情况下不能替代其他层面的鉴别。	正确	错误		
4715	判断题	如果将密钥以密文形式存放在数据库中，对其采用SM4-GCM保护机密性和完整性即可，无需对密钥密文和用户的关联关系进行完整性保护。	正确	错误		
4716	判断题	只需要对口令进行HMAC-SM3计算，就可以保证口令不被替换，实现实体与口令的绑定。	正确	错误		
4717	判断题	在测评时发现系统数据库中存储的用户口令是加盐存储的，盐值采用的策略是每100个用户换一个盐值的方式，该实现是安全的。	正确	错误		
4718	判断题	某部署在运营商机房的信息系统，其物理机房完全由运营商托管，那么对该信息系统进行密评时，物理和环境安全层面视为“不适用”。	正确	错误		
4719	判断题	某信息系统网络通道仅采用HTTP协议传输报文，但该通道中传输的数据在应用和数据安全层面采用密码技术进行保护，“重要数据传输机密性”“重要数据传输完整性”这两项指标中得到“符合”的判定结果。那么“通信过程中重要数据的机密性”的安全风险等级可以酌情降低。	正确	错误		
4720	判断题	开展信息系统密评时，“设备远程管理通道安全”测评项可能涉及“网络和通信安全”和“设备和计算安全”两个层面。	正确	错误		

4721	判断题	在密评中发现，信息系统采用一台服务器密码机实现对数据加密密钥的管理，但该密码机对应的产品认证证书在测评时已过期（该密码机采购时间在认证证书有效期内）。针对这种情形，“密钥管理安全性”一定是“不符合”。	正确	错误		
4722	判断题	在应用和数据安全层面，某信息系统开发人员对重要数据的传输机密性保护采用AES-CBC实现，对重要数据的传输完整性保护采用基于AES的CBC-MAC实现，由于这两项指标对应保护的数据不同，因此开发人员使用了同一个密钥执行上述密码算法计算。这种做法是合理的。	正确	错误		
4723	判断题	由于防火墙、边界路由器属于网络安全产品范畴，在密评时通常不考虑作为测评对象。所以“网络边界访问控制信息的完整性”测评指标的核查只需要确认VPN网关中相应的安全机制即可。	正确	错误		
4724	判断题	某信息系统的设备运维路径为：设备管理员操作终端-堡垒机-应用服务器，其中：1）从操作终端到堡垒机采用HTTPS/TLS1.2（选用密码套件为TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384）提供运维通道保护；2）从堡垒机到服务器采用SSHv2.0提供运维通道保护。 那么应用服务器的“远程管理通道安全”测评指标的判定结果为“部分符合”。	正确	错误		

4725	判断题	密评人员在测评某信息系统应用和数据安全层面的“身份鉴别”指标时发现，该信息系统有应用管理员和普通用户两类应用用户，其中应用管理员采用基于智能密码钥匙（经检测认证合格）的登录方式，普通用户采用“口令+短信验证码”的登录方式。那么该测评单元的得分为0.5分。	正确	错误		
4726	判断题	测评人员利用Wireshark，发现某信息系统传输的重要数据为密文，数据密文长度为128比特，因此可以判定该数据使用SM4或AES密码算法进行了加密保护。	正确	错误		
4727	判断题	在对物理和环境安全层面中的“身份鉴别”指标测评时，如果被测信息系统所在物理机房未采用密码技术对机房进入人员进行身份鉴别，但在机房进出口配备专人值守并进行登记，且采用视频监控系统进行实施监控保证机房进入人员身份的真实性，可酌情降低风险等级，但该测评指标的量化评估分数依然是0分。	正确	错误		
4728	判断题	测评人员在对某三级信息系统测评时，发现该信息系统运行过程中未发生任何密码应用安全事件，因此将GB/T 39786中管理要求的“应急处置”相关指标列为不适用。	正确	错误		
4729	判断题	测评人员对某一级信息系统测评时，发现该系统在规划阶段制定了密码应用方案且通过了方案评估，因此针对“建设运行”层面的“制定密码应用方案”指标的量化评估结果可以为1分，判定为符合。	正确	错误		

4730	判断题	某二级信息系统除了灾备机房外，其中一部分部署在被测系统单位内机房，另一部分部署在云平台（由运营商托管），那么针对“物理和环境安全”层面的测评对象仅涉及灾备机房和被测系统单位内机房。	正确	错误		
4731	判断题	某二级信息系统于2019年进行规划并有密码应用方案且方案通过评估，2020年建设完成后投入运行，2021年开展首次密评，测评人员在测评时仅以该系统在投入运行前未进行密码应用安全性评估为由，对“建设运行”层面的“投入运行前进行密码应用安全性评估”指标判定为“不符合”。	正确	错误		
4732	判断题	测评人员在对某四级信息系统进行测评时，核实该信息系统所属机构建立了密码应用岗位责任制度，设置了密钥管理员、密码安全审计员、密码操作员，其中密钥管理员和密码安全审计员均由被测系统所属机构内部人员担任，密码操作员由被测系统承包商担任，且密码安全审计员与密钥管理员、密码操作员为不同人员，因此针对“人员管理”层面的“建立密码应用岗位责任制度”指标可以判定为符合。	正确	错误		
4733	判断题	某三级信息系统所在机房部署符合GM/T 0036《采用非接触卡的门禁系统密码应用指南》的电子门禁系统，使用SM4算法进行密钥分散，实现门禁卡的“一卡一密”，并基于SM4算法对人员身份进行鉴别，因此该系统在“物理和环境安全”层面的“电子门禁记录数据存储完整性”指标可以判定为符合。	正确	错误		

4734	判断题	某三级信息系统的系统管理员通过堡垒机对通用服务器进行远程管理，系统管理员登录堡垒机时通过检测认证合格的安全浏览器和智能密码钥匙并基于数字证书的方式进行身份鉴别，数字签名算法为SM2，因此该信息系统在“设备和计算安全”层面的通用服务器测评对象的“身份鉴别”指标可以判定为符合。	正确	错误		
4735	判断题	某三级信息系统使用云服务器密码机对云平台内的数据进行保护，测评人员在对云服务器密码机进行测评时，发现云服务器密码机的宿主机和三个虚拟机密码机均有独立的管理界面，并通过同一管理员进行管理，管理员登录前基于合规的密码技术进行了身份鉴别。因此，对于虚拟机密码机，针对“设备和计算安全”层面的“身份鉴别”指标量化评估结果为1分。	正确	错误		
4736	判断题	测评人员发现，某二级信息系统系统未使用任何密码技术和密码产品对系统相关的物理和环境、网络和通信、设备和计算、应用和数据安全层面进行防护。鉴于系统不涉及任何密码技术和密码产品，因此将“管理制度”层面的测评指标列为不适用。	正确	错误		
4737	判断题	“密码算法和密码技术合规性”测评单元在测评时，需要汇集信息系统所有密码算法和密码技术，逐个分析其合规性，给出相应量化评估分数。	正确	错误		

4738	判断题	判断以下做法是否正确：用户身份鉴别完成后，用户利用签名私钥与信息系统进行SM2密钥协商，协商出会话密钥，利用SM4算法和基于SM3的HMAC算法进行通信数据的机密性和完整性保护。	正确	错误		
4739	判断题	判断以下做法是否正确：用户在生成SM2签名密钥对时，以当前时间为种子，利用C语言的rand函数生成随机数；为了保证随机数的随机性，将该随机数再利用SHA-256算法进行杂凑计算，获得256比特数据作为私钥，并生成对应公钥。	正确	错误		
4740	判断题	某信息系统的设备运维路径为：设备管理员终端-堡垒机-通用设备。其中，堡垒机的“身份鉴别”指标的测评结果为“符合”，那么通用设备（自身采用“用户名+口令”方式登录）的“身份鉴别”指标的量化评估分值可以一定程度上得到弥补。	正确	错误		
4741	判断题	某三级信息系统使用服务器密码机（经检测认证合格）对应用的重要数据进行存储机密性保护，针对该服务器密码机的“设备和计算安全”层面的“身份鉴别”指标可以直接判定为符合。	正确	错误		

4742	判断题	某三级信息系统有两个独立的物理机房，其中机房1采用门禁ID卡对进入人员进行身份鉴别；机房2有两个门，其中门A采用门禁ID卡对进入人员进行身份鉴别，门B通过部署符合GM/T 0036《采用非接触卡的门禁系统密码应用技术指南》的电子门禁系统对进入人员进行身份鉴别。针对“物理和环境安全”层面的“身份鉴别”指标，机房1的量化评估结果为0分，机房2的量化评估结果为0分。	正确	错误		
4743	判断题	测评人员在对某三级信息系统的人员管理中的“建立密码应用岗位责任制度”测评时发现，该信息系统根据密码应用的实际情况，设置甲、乙、丙三人分别担任密钥管理员、密码安全审计员、密码操作员，并建立了岗位责任制度、确定了各自的岗位职责，设备与系统的管理和使用人员都有各自单独的账号。因此，该测评项可以给1分。	正确	错误		
4744	单项选择题	根据《商用密码应用安全性评估报告模板（2023版）》，关于方案密评，以下说法那种不正确（）。	重点判断系统在某方面是否存在安全风险，通过总体密码设计是否可以有效解决相应的安全问题	重点对所有自查符合性进行评估，对所有自查不适用项和对应论证依据进行逐条核查、评估	应注意梳理安全需求，尤其是应用和数据安全层面各保护对象的安全需求	重点是对照GB/T 39786-2021《信息安全技术 信息系统密码应用基本要求》进行逐条评估
4745	单项选择题	根据《商用密码应用安全性评估报告模板（2023版）》，以下哪项不属于方案密评报告所包含的内容（）。	报告分发范围	密码应用方案	密评委托证明	测评人员进入系统所在机房的证明记录

4746	单项选择题	根据《商用密码应用安全性评估报告模板（2023版）》，在方案密评报告的“商用密码应用安全性评估结论”部分不包括以下哪项（）。	方案名称	评估结论	不适用指标数目	密码应用需求
4747	单项选择题	根据《商用密码应用安全性评估报告模板（2023版）》，密码应用方案密评报告中的商用密码应用安全性评估结论部分包含哪项要素（）。	方案名称和评估结论	方案简介和评估情况简介	不适用项数目/总测评指标项数目	以上均包含
4748	单项选择题	根据《商用密码应用安全性评估报告模板（2023版）》，系统概述部分不需要对应用和数据安全层面的哪些保护对象做梳理（）。	应用系统的用户	重要数据	用户操作行为	网络通道
4749	单项选择题	根据《商用密码应用安全性评估报告模板（2023版）》，以下哪项信息系统内的资产不属于需要梳理的对象（）。	交换机	机房	密码设备	服务器
4750	单项选择题	根据《商用密码应用安全性评估报告模板（2023版）》，编制方案密评报告时，以下对于不适用指标描述不合理的是（）。	信息系统不涉及设备中的重要信息资源安全标记，因此设备和计算安全层面的“重要信息资源安全标记完整性”指标为不适用	信息系统中重要数据仅有完整性安全需求，不存在机密性安全需求，因此应用和数据安全层面的“重要数据传输和存储机密性”指标为不适用	信息系统的物理机房难以进行密码改造，因此物理和环境安全层面的“身份鉴别”指标为不适用	信息系统责任单位将“可”的指标自行决定为不适用

4751	单项选择题	根据《商用密码应用安全性评估报告模板（2023版）》，针对“安全控制措施评估结果”环节的工作，以下描述较为合理的是（ ）。	某三级信息系统密码应用方案中，针对应用和数据安全层面的重要数据传输保护均使用国外密码算法，因此“重要数据传输机密性和完整性”指标的安全控制措施评估结果为“未通过”	某三级信息系统41个基本指标中，其中一个指标的安全控制措施评估结果为“未通过”，因此该信息系统的密码应用方案评估结果为“不通过”	某三级信息系统密码应用方案的安全控制措施评估结果均为“通过”，初步量化评估分值为50分，那么该密码应用方案的整体评估结果仍可为“通过”	某三级信息系统密码应用方案中，针对物理和环境安全层面的“身份鉴别”指标未采用密码技术方案，而是通过其他的安全管理措施降低风险，因此该指标的安全控制措施评估结果一定为“未通过”
4752	单项选择题	根据《商用密码应用安全性评估报告模板（2023版）》，如果应用和数据安全层面的“重要数据存储完整性”指标未采用密码应用措施，那么针对该指标的安全控制措施评估结果一定是（ ）。	通过	未通过	不符合	无法判断
4753	单项选择题	根据《商用密码应用安全性评估报告模板（2023版）》，对于委托第三方密评机构实施的密码应用方案密评和信息系统密评的情形，在报告中的“密评活动有效性证明”记录部分，以下说法正确的是（ ）。	信息系统密评报告需要提供密评活动证明，方案密评报告则不需要	信息系统密评时，测评方案需要测评委托方和密评机构双方签字确认，同时需要密评机构内部组织评审	方案密评前，应编制测评方案，并对该方案组织内部评审	信息系统密评时，测评方案需要测评委托方和密评机构双方签字确认，但不需要密评机构内部组织评审
4754	单项选择题	根据《商用密码应用安全性评估报告模板（2023版）》，在密码应用方案密评报告附录部分，“密评活动有效性证明记录”不涉及（ ）。	密评委托证明	密评人员差旅票证及住宿票证	密评报告评审记录	密评人员资格情况
4755	多项选择题	根据《商用密码应用安全性评估报告模板（2023版）》，在密码应用方案密评报告中，在应用和数据安全层面“保护对象”表中应重点梳理信息系统中（ ）。	各个应用中具有身份鉴别（真实性）需求的应用用户类型	各个应用的重要数据及对应具体安全需求	各个应用承载业务情况	各个应用具有不可否认性需求的操作行为

4756	多项选择题	根据《商用密码应用安全性评估报告模板（2023版）》，关于方案密评，以下说法正确的是（）。	依据被测信息系统具体业务情况，审查被测信息系统的密码应用方案是否涵盖了所有需要采用密码保护的核心资产	依据被测信息系统具体业务情况，审查被测信息系统的密码应用方案是否涵盖了所有需要采用密码保护的敏感信息	依据被测信息系统具体业务情况，审查被测信息系统的密码应用方案采取的密码保护措施是否均能够达到相应等级的密码使用要求或规定	方案密评可由信息系统责任单位委托密评机构或自行开展密评
4757	多项选择题	根据《商用密码应用安全性评估报告模板（2023版）》，密码应用方案的“背景”部分可包含（）。	系统的建设规划	国家有关法律法规的要求	与规划相关的前期情况概述	项目实施的必要性
4758	多项选择题	根据《商用密码应用安全性评估报告模板（2023版）》，在编写密码应用方案时，应该体现（）。	系统承载业务情况及网络拓扑	系统密码应用需求分析	各安全层面的技术实现方案	安全与和合规性分析
4759	多项选择题	根据《商用密码应用安全性评估报告模板（2023版）》，下列关于密码应用方案的说法中，错误的是（）。	密码应用方案及其评估意见是判定GB/T 39786《信息安全技术 信息系统密码应用基本要求》中“宜”是否适用的重要依据	对于部署在同一云平台上的云上应用，虽然网络安全等级保护定级时进行了独立定级，考虑到其物理环境、通信信道、系统资产等方面的共用的软硬件比较多，可以编写一份密码应用方案统一进行密码应用分析	如密码应用方案中对被测信息系统对测评单元“不可否认性”进行了不适用判定，但在执行现场测评过程中，系统责任单位向密评机构反映系统实际存在不可否认性密码应用需求，应根据通过评估的密码应用方案，对该测评项进行不适用判定	密码应用方案中应详细梳理应用的业务流程及业务数据，根据流程安全需求及数据安全需求，为重要流程及重要数据设计保护机制

4760	多项选择题	根据《商用密码应用安全性评估报告模板（2023版）》，方案密评报告的评估结论包括（ ）。	符合	不符合	通过	不通过
4761	多项选择题	根据《商用密码应用安全性评估报告模板（2023版）》，方案密评报告中系统概述部分内容应包含（ ）。	系统网络拓扑	承载的业务情况	各安全层面保护对象	项目情况
4762	多项选择题	根据《商用密码应用安全性评估报告模板（2023版）》，系统概述部分需要结合系统网络拓扑图描述（ ）。	物理机房的个数及其所在具体位置	网络边界划分以及与其他系统的互联关系	跨网络访问的通信信道	设备组成及实现功能
4763	多项选择题	根据《商用密码应用安全性评估报告模板（2023版）》，方案密评报告中应用和数据安全层面的保护对象应重点梳理（ ）。	各个应用具有身份鉴别需求的应用用户	各个应用具有可用性需求的重要数据	各个应用的重要数据及对应具体安全需求	各个应用具有不可否认性需求的操作行为
4764	多项选择题	根据《商用密码应用安全性评估报告模板（2023版）》，方案评估报告在“管理制度”方面，关注重点通常包括（ ）。	安全管理制度类文档	密码应用方案	密钥管理制度及策略类文档	系统相关人员
4765	多项选择题	根据《商用密码应用安全性评估报告模板（2023版）》，方案评估报告在“建设运行”方面，关注重点通常包括（ ）。	密码应用方案	密钥管理制度	攻防对抗演习报告	密码应用安全管理制度
4766	多项选择题	根据《商用密码应用安全性评估报告模板（2023版）》，方案评估报告在“人员管理”方面，关注重点通常包括（ ）。	安全管理制度类文档	记录表单类文档	系统相关人员	整改文档
4767	多项选择题	根据《商用密码应用安全性评估报告模板（2023版）》，方案评估报告在“应急处置”方面，关注重点通常包括（ ）。	密码应用应急处置方案	应急处置记录类文档	安全事件发生情况及处置情况报告	系统相关人员
4768	多项选择题	根据《商用密码应用安全性评估报告模板（2023版）》，系统各安全层面需要梳理的保护对象不包括（ ）。	网络和通信安全层面的通信信道	不同应用用户	重要数据	通用交换机

4769	多项选择题	根据《商用密码应用安全性评估报告模板（2023版）》，在密码应用方案密评报告中，“安全控制措施描述及指标适用情况”章节的“指标适用情况及论证说明”部分，应体现的内容包括（ ）。	各测评项的测评指标适用情况	不适用项的不适用性论证说明	测评项中存在部分保护对象不适用情况的不适用性论证说明	不适用指标合计项数
4770	多项选择题	《商用密码应用安全性评估报告模板（2023版）》中在描述安全控制措施时，需要注意的事项有（ ）。	安全控制措施需要包括四个密码应用技术层面和四个密码应用管理方面的内容	如果相关保护对象未采用密码技术措施，那么也需要概括总结相关的风险替代措施	安全控制措施描述需要结合信息系统的密码应用部署图	系统密码应用部署图中需要包含密码应用方案中涉及的所有密码产品（冗余配置的除外）和服务
4771	多项选择题	根据《商用密码应用安全性评估报告模板（2023版）》，某三级信息系统密码应用方案的评估结论为“不通过”，最可能原因包括（ ）。	采用的安全控制措施仍会导致高风险项存在	初步量化评估未达到阈值要求	密码应用方案中不适用指标项数过多	密码应用方案有较多冗余内容
4772	多项选择题	根据《商用密码应用安全性评估报告模板（2023版）》，“指标适用情况及论证说明”表格中不涵盖（ ）。	密码算法	密码技术	密码产品	密码服务
4773	多项选择题	根据《商用密码应用安全性评估报告模板（2023版）》，编制方案密评报告时，以下属于风险替代措施的是（ ）。	机房采用人脸+指纹识别的方式对进人人员进行身份鉴别	通用服务器采用指纹的方式对登录设备用户进行身份鉴别	业务应用采用人脸识别+短信验证码的方式对登录人员进行身份鉴别	应用层采用了合规的密码技术对传输数据进行机密性和完整性保护
4774	多项选择题	根据《商用密码应用安全性评估报告模板（2023版）》，不同安全层面指标的安全控制措施的评估结果可能是（ ）。	通过	未通过	符合	不符合

4775	多项选择题	根据《商用密码应用安全性评估报告模板（2023版）》，针对安全控制措施评估，以下描述不合理的是（ ）。	某三级信息系统密码应用方案中，针对网络和通信安全层面的通信数据传输保护均使用国外密码算法，则“通信数据传输机密性和完整性”指标的安全控制措施评估结果仍可能为“通过”	某三级信息系统41个基本指标中，仅有一个指标的安全控制措施评估结果为“未通过”，因此该密码应用方案评估结果为“通过”	某三级信息系统密码应用方案的安全控制措施评估结果中，其中1项为未通过，但初步量化评估分值为75分，因此该密码应用方案的整体评估结果为“通过”	某三级信息系统密码应用方案中，针对物理和环境安全层面的“身份鉴别”指标未采用密码技术方案，而是通过其他的安全管理措施降低风险，因此该指标的安全控制措施评估结果为“未通过”

4776	多项选择题	根据《商用密码应用安全性评估报告模板（2023版）》，密评人员对密码应用方案中的安全控制措施分析和评估结果判定不合理的是（）。	针对物理和环境安全层面，密码应用方案中的描述为“机房虽采用门禁ID卡刷卡进入，但机房门外部署有视频监控系统，能够对机房外的环境进行实时监控，因此不存在高风险”，针对物理和环境安全层面“身份鉴别”的安全控制措施评估结果为“通过”	针对网络和通信安全层面，密码应用方案中的描述为“虽然互联网PC端与系统服务端在通信时未采用密码技术对服务端进行身份鉴别，但是系统应用层对登录用户采用合规的密码技术进行身份鉴别，因此网络通信实体的身份鉴别问题不存在高风险”，针对网络和通信安全层面“身份鉴别”的安全控制措施评估结果为“通过”	针对应用和数据安全层面，密码应用方案中的描述为“虽然未采用密码技术对重要数据做存储机密性保护，但是数据库只能专人访问，且登录口令定期更换，因此不存在高风险”，针对“重要数据存储机密性”的安全控制措施评估结果为“通过”	针对应用和数据安全层面，密码应用方案中的描述为“虽然未采用密码技术对存储的业务数据进行完整性保护，但是应用系统具有符合要求的身份鉴别措施，只有授权人员才能访问应用系统的重要数据，且定期对数据进行备份，因此不存在高风险”，针对“重要数据存储完整性”的安全控制措施评估结果为“通过”
4777	多项选择题	根据《商用密码应用安全性评估报告模板（2023版）》，下列关于密码应用方案密评报告和信息系统密评报告的说法中，错误的是（）。	根据“三同步一评估”的要求，在规划阶段，评估对象是信息系统的密码应用方案，在建设和运行阶段，评估对象是实际的信息系统	密码应用方案密评的评估结论中，可能存在“通过”和“不通过”判定，也可能存在“修改后通过”的判定	在对密码应用方案进行密评时，如初步量化评估分数达到了阈值的要求，则方案评估结论即可为“通过”	信息系统密评报告中的“检测结果记录”中，“安全管理”层面的测评单元得分仅可能为1分、0.5分和0分

4778	多项选择题	根据《商用密码应用安全性评估报告模板（2023版）》，在方案密评报告中，以下可判定某指标的评估结果为“通过”的情况有（ ）。	该指标涉及的所有保护对象不涉及高风险	该指标涉及的所有保护对象的风险替代措施均有效	该指标涉及的所有保护对象的密码应用措施均有效，不涉及高风险，且方案中描述的实施保障措施合理	该指标涉及的所有保护对象的风险替代措施均有效，不涉及高风险，且方案中描述的实施保障措施合理
4779	多项选择题	根据《商用密码应用安全性评估报告模板（2023版）》，密码应用方案密评报告“密评活动证明”部分，一般作为活动证明的证明材料包括（ ）。	电子邮件	通话记录	会议记录	系统现场测评记录
4780	多项选择题	根据《商用密码应用安全性评估报告模板（2023版）》，方案密评报告中系统承载业务情况应包含（ ）。	业务应用	业务功能	应用用户	重要数据以及关键的用户操作行为等
4781	判断题	根据《商用密码应用安全性评估报告模板（2023版）》，方案评估工作完成后，当被评估的《XXX系统密码应用方案》发生变更时，已出具的方案评估报告仍然适用。	正确	错误		
4782	判断题	根据《商用密码应用安全性评估报告模板（2023版）》，对于密码应用方案已通过评估的系统，密评时应把方案作为测评的重要依据。	正确	错误		
4783	判断题	根据《商用密码应用安全性评估报告模板（2023版）》，对于已建但尚未规划密码方案的系统，信息系统责任单位应通过调研分析，梳理形成系统当前密码应用的总体架构图，提炼出密码应用情况，作为后续测评实施的基础。	正确	错误		

4784	判断题	根据《商用密码应用安全性评估报告模板（2023版）》，方案密评主要工作是对照GB/T 39786《信息安全技术 信息系统密码应用基本要求》进行逐条评估，而不是对信息系统中安全控制措施和指标适用情况梳理。	正确	错误		
4785	判断题	根据《商用密码应用安全性评估报告模板（2023版）》，只需要在报告中阐述每个安全层面中各个保护对象的密码应用措施，其他非密码技术的安全控制措施无需描述。	正确	错误		
4786	判断题	根据《商用密码应用安全性评估报告模板（2023版）》，在密码应用方案密评报告中，仅在报告中体现密评机构针对系统责任单位编写的密码应用方案进行密评的合规性判定情况即可，无需附上密码应用方案。	正确	错误		
4787	判断题	根据《商用密码应用安全性评估报告模板（2023版）》，在密码应用方案中对指标适用情况及论证说明时，应对不适用部分做出相应的原因论述，体现出能够降低风险的措施。	正确	错误		
4788	判断题	根据《商用密码应用安全性评估报告模板（2023版）》，密码应用方案密评结果不需要进行密评结果备案，仅系统密评结果需要进行密评结果备案。	正确	错误		
4789	判断题	根据《商用密码应用安全性评估报告模板（2023版）》，方案评估报告中给出的评估结论仅对报告所附《XXX系统密码应用方案》的内容有效。	正确	错误		

4790	判断题	根据《商用密码应用安全性评估报告模板（2023版）》，方案评估报告可适用于实际建设的系统评估结论。	正确	错误		
4791	判断题	根据《商用密码应用安全性评估报告模板（2023版）》，方案评估结论不能作为运行系统的评估结论。	正确	错误		
4792	判断题	根据《商用密码应用安全性评估报告模板（2023版）》，方案密评报告中的安全控制措施评估结果可以直接在系统密评报告中复用。	正确	错误		
4793	判断题	根据《商用密码应用安全性评估报告模板（2023版）》，针对选定的密评指标，方案密评报告评估结果为“通过/未通过”，系统密评报告的评估结果为“符合/部分符合/不符合/不适用”。	正确	错误		
4794	判断题	根据《商用密码应用安全性评估报告模板（2023版）》，方案密评报告中信息系统承载的业务情况应重点说明业务的保护对象和资产情况。	正确	错误		
4795	判断题	根据《商用密码应用安全性评估报告模板（2023版）》，应用和数据安全层面需要进一步梳理各个应用的保护对象（如应用用户、重要数据）及保护对象的相应安全需求。	正确	错误		
4796	判断题	根据《商用密码应用安全性评估报告模板（2023版）》，在“指标适用情况及论证说明部分”，即便指标为适用，也可能存在部分保护对象不适用的情况，需要在方案评估报告中给出相关保护对象不适用性的论证说明。	正确	错误		

4797	判断题	根据《商用密码应用安全性评估报告模板（2023版）》，在密码应用方案密评报告中，不适用指标的合计项数中不应计入存在部分保护对象不适用情况的测评项。	正确	错误		
4798	判断题	根据《商用密码应用安全性评估报告模板（2023版）》，不同安全层面指标的安全控制措施评估结果有符合、不符合、部分符合三种情况。	正确	错误		
4799	判断题	根据《商用密码应用安全性评估报告模板（2023版）》，如果指标所涉及的某一保护对象的相应安全控制措施有效（不存在高风险），则该指标的安全控制措施评估结果为“通过”。	正确	错误		
4800	判断题	根据《商用密码应用安全性评估报告模板（2023版）》，针对应用和数据安全层面的“重要数据传输完整性”指标，如果未采用密码应用措施，那么针对该指标的安全控制措施评估结果一定是“未通过”。	正确	错误		
4801	判断题	某三级信息系统在密码应用方案中针对物理和环境安全给出的安全控制措施为：信息系统所在物理机房使用门禁ID卡+指纹识别的方式对进入机房人员进行身份鉴别，同时机房外有24小时专人值守，并在机房内外部署了视频监控系统。根据《商用密码应用安全性评估报告模板（2023版）》，针对物理和环境安全层面的“身份鉴别”指标的安全控制措施评估结果为“通过”。	正确	错误		

4802	判断题	某四级信息系统在密码应用方案中，针对应用和数据安全层面的“重要数据存储机密性、存储完整性”指标分别给出如下安全控制措施：重要业务数据均采用DES算法进行存储机密性保护，使用基于SM3的HMAC算法进行存储完整性保护。根据《商用密码应用安全性评估报告模板（2023版）》，该密码应用方案的评估结论很可能是“不通过”。	正确	错误		
4803	判断题	根据《商用密码应用安全性评估报告模板（2023版）》，如果信息系统密码应用方案中针对各个层面的保护对象的安全控制措施评估结果为“通过”，那么该系统的密评结果一定是“符合”。	正确	错误		
4804	判断题	根据《商用密码应用安全性评估报告模板（2023版）》，在密码应用方案密评报告中，所有指标的安全控制措施评估结果均通过，则可判定方案评估结论为“通过”。	正确	错误		
4805	判断题	根据《商用密码应用安全性评估报告模板（2023版）》，在密码应用方案密评报告和信息系统密评报告中，均需体现被测系统的网络安全等级保护定级备案名称、备案时间及等保定级备案证明。	正确	错误		