2025 年江苏省密码行业
职业技能竞赛题库

竞赛组委会

2025 年 9 月

目录

政策法规及技术标准范围

政策法规：《中华人民共和国密码法》、《中华人民共和国网络安全法》、《中华人民共和国个人信息保护法》、《中华人民共和国数据安全法》、《中华人民共和国电子签名法》、《商用密码管理条例》、《网络安全审查办法》、《商用密码检测机构管理办法》、《商用密码应用安全性评估管理办法》、《电子政务电子认证服务管理办法》、《关键信息基础设施商用密码使用管理规定》、《江苏省省级政务信息化项目建设管理办法》、《国家政务信息化项目建设管理办法》、《江苏省数据条例》等；

技术标准：GB/T 39786-2021《信息安全技术 信息系统密码应用基本要求》、GB/T 43207-2023《信息安全技术 信息系统密码应用设计指南》、GB/T 33560-2017《信息安全技术 密码应用标识规范》、GB/T 20986-2023《信息安全技术 网络安全事件分类分级指南》、GB/T 20984-2022《信息安全技术 信息安全风险评估方法》、GM/Z 4001-2013《密码术语》、GM/T 0014-2023《数字证书认证系统密码协议规范》、GM/T 0021-2023《动态口令密码应用技术规范》、GM/T 0028-2024《密码模块安全技术要求》、GM/T 0036-2014《采用非接触卡的门禁系统密码应用技术指南》、GM/T 0037-2014《证书认证系统检测规范》、GM/T 0039-2024《密码模块安全检测要求》、GM/T 0116-2021《信息系统密码应用测评过程指南》、GM/T 0133-2024《关键信息基础设施密码应用要求》、GM/T 0134-2024《密码模块安全设计指南》、GM/T 0139-2024《信息系统密码应用安全管理体系》，以及 ZUC、SM2、SM3、SM4、SM9 国产密码算法等技术标准。

第一部分基础题 250

一、密码法律法规 80

一、单选题 50

1. 依据《中华人民共和国密码法》，（　　）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，（　　）应当配合。

A、中央密码工作领导机构、密码管理部门

B、密码管理部门、密码工作机构

C、中央密码工作领导机构、密码工作机构

D、密码管理部门、保密行政管理部门

答案：B

2. 核心密码、普通密码属于国家秘密。（　　）依照《中华人民共和国密码法》和有关法律、行政法规、国家有关规定对核心密码、普通密码实行严格统一管理。

A、保密行政管理部门

B、密码管理部门

C、中央密码工作领导机构

D、密码工作机构

答案：B

3. 某公司开发了一套系统用于项目管理，系统中存放了公司的核心业务数据，公司领导人希望对其进行加密存储。依据《中华人民共和国密码法》，应使用（　　）进行保护。

A、核心密码

B、普通密码

C、一般密码

D、商用密码

答案：D

4. （　　）是我国密码工作最重要、最根本、最核心的原则。

A、坚持总体国家安全观

B、坚持中央密码工作领导机构的统一领导

C、坚持党的领导

D、坚持集中统一领导

答案：C

5. 关于国家密码管理局的主要职责，下列说法错误的是（　　）。

A、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

B、指导密码专业教育和密码学术交流

C、承办中央保密委员会的部分工作

D、起草密码工作法规并负责密码法规的解释

答案：C

6. 《中华人民共和国密码法》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。

A、加密保护、安全认证
B、加密保护
C、安全认证
D、匿名保护
答案：A

7. 下列哪项不属于《中华人民共和国密码法》规范的密码（　　）。
A、基于格的密码
B、支付宝登录口令
C、抗量子密码
D、税票防伪标识符的加密算法
答案：B

8. 根据《中华人民共和国密码法》，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。
A、总体国家安全观
B、整体国家安全观
C、综合国家安全观
D、安全发展观
答案：A

9. 根据《中华人民共和国密码法》，以下哪类密码需要实行严格统一管理（　　）。
A、核心密码
B、商用密码产品
C、商用密码技术
D、商用密码服务
答案：A

10. 关于《中华人民共和国密码法》，下列说法错误的是（　　）。
A、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
B、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
C、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
D、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
答案：D

11. 根据《中华人民共和国密码法》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。
A、核心密码
B、普通密码
C、商用密码
D、民用密码
答案：C

12. 根据《中华人民共和国密码法》，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。

A、人才培养，突出贡献
B、教育培训，突出成绩
C、人员素质，卓越贡献
D、教育培训，突出贡献
答案：A

13. 根据《中华人民共和国密码法》，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。
A、9 年义务教育体系和国民教育体系
B、国民教育体系和公务员教育培训体系
C、公务员教育体系和成人教育体系
D、成人教育体系和九年义务教育体系
答案：B

14. 根据《中华人民共和国密码法》，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。
A、安全监测预警、安全风险评估、信息通报、重大事项会商
B、安全监测预警、安全风险评估、重大事项会商
C、安全监测预警、信息共享、重大事项会商
D、安全风险评估、事件报告、重大事项会商
答案：A

15. 根据《中华人民共和国密码法》，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（　　）。
A、立即采取措施
B、及时向保密行政管理部门报告
C、及时向密码管理部门报告
D、以上都是
答案：D

16. 根据《中华人民共和国密码法》，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。
A、开放原则
B、平等原则
C、自愿原则
D、非歧视原则
答案：D

17. 国家为了增强密码安全保障能力，加强核心密码、普通密码的科学规划、管理和使用，以下哪种情形应使用核心密码、普通密码进行加密保护、安全认证？（　　）
A、某公司在无线通信中传递商业机密
B、对某系统存储的大量个人信息进行加密
C、某单位在有线通信中传递国家秘密信息
D、张某利用 VPN 传递学习资料

答案：C

18. 根据《中华人民共和国密码法》，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。
A、低于
B、多于
C、高于
D、相当于
答案：C

19. 《中华人民共和国密码法》明确了商用密码检测认证制度，下列说法正确的是（　　）。
A、目前我国采用的是商用密码产品品种和型号审批
B、商用密码服务使用网络关键设备的，实行自愿认证
C、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
D、在商用密码检测认证中，自愿检测认证成为主要方式
答案：D

20. 根据《中华人民共和国密码法》，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。
A、关键信息基础设施国家安全审查
B、网络安全风险评估
C、关键信息基础设施安全检测评估
D、网络安全检测、认证
答案：C

21. 《中华人民共和国密码法》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（　　）。
A、该制度是《中华人民共和国网络安全法》规定的网络安全审查的一部分
B、该制度由国家安全部门单独落实
C、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
D、该制度与《中华人民共和国国家安全法》规定的国家安全审查制度是两个独立制度
答案：A

22. 根据《中华人民共和国密码法》，实施进口许可的商用密码应符合的条件是（　　）。
A、涉及国家安全且具有安全认证功能
B、涉及社会公共利益且具有安全认证功能
C、中国承担国际义务
D、涉及国家安全、社会公共利益且具有加密保护功能
答案：D

23. 根据《中华人民共和国密码法》，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。
A、电子数据
B、电子签名
C、电子文档
D、电子证照
答案：B

24. 根据《中华人民共和国密码法》，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。
A、保密行政管理部门
B、密码管理部门
C、保密行政管理部门、密码管理部门
D、国家安全部门
答案：C

25. 《中华人民共和国密码法》的正式施行日期是（　　）。
A、2020 年 1 月 1 日
B、2021 年 1 月 1 日
C、2020 年 6 月 1 日
D、2019 年 10 月 26 日
答案：A

26. 根据《中华人民共和国密码法》，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（　　）。
A、商用密码检测认证中，自愿检测认证是主要方式
B、商用密码检测认证中，强制检测认证是主要方式
C、商用密码检测、认证机构资质由国家密码管理局单独管理
D、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
答案：A

27. 根据《中华人民共和国密码法》，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（　　）。
A、供涉密单位使用
B、能轻易改变密码功能
C、通过常规零售渠道购买会受到一定的限制
D、对国家安全带来的风险较小且可控
答案：D

28. 根据《中华人民共和国密码法》，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（　　）。
A、一定程度上与电子认证服务机构存在重复许可
B、与电子认证服务机构的审批对象一致
C、可适用于电子商务领域的电子认证服务机构
D、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

答案：D

29. 根据《中华人民共和国密码法》，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（ ）。
A、只有经营性企业
B、不包括提供公共服务的事业单位
C、只包括提供公共服务的事业单位
D、包括经营性企业和提供公共服务的事业单位
答案：D

30. 根据《中华人民共和国密码法》，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（ ）。
A、实施违法行为中起决定作用的人
B、实施违法行为中起指挥作用的人
C、授意实施违法行为的人
D、具体实施违法行为并起较大作用的人
答案：D

31. 国家鼓励和促进商用密码产业发展，依据（ ），各级人民政府及其有关部门应以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。
A. 《中华人民共和国密码法》
B. 《中华人民共和国数据安全法》
C. 《中华人民共和国网络安全法》
D. 《商用密码管理条例》
答案：A

32. 根据《中华人民共和国密码法》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，并会同有关部门负责政务活动中使用（ ）的管理。
A、电子签名和数据电文
B、电子文档和电子证照
C、电子印章和数字证书
D、电子档案和电子合同
答案：A

33. 依据《中华人民共和国密码法》涉及国家安全、国计民生、社会公共利益的商用密码产品，在销售或提供前必须满足的法定要求是（ ）。
A、通过企业自检并公开声明符合标准
B、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
C、获得国际标准化组织（ISO）认证
D、获得地方市场监管部门认可并备案
答案：B

34. 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，其主要目的是（　）。
A、降低国内商用密码产品的生产成本
B、推进商用密码中国标准与国外标准之间的转化运用
C、限制外资企业参与国际标准制定
D、强制推广中国商用密码标准至其他国家
答案：B

35. 依据《中华人民共和国密码法》，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（　）等密码相关专有信息。
A、产品型号
B、源代码
C、产品厂商
D、技术标准
答案：B

36. 根据《商用密码管理条例》，商用密码的保护对象是（　）。
A、国家秘密信息
B、非国家秘密信息
C、所有网络信息
D、仅限金融领域数据
答案：B

37. 《商用密码管理条例》要求电子政务电子认证服务机构必须具备（　）。
A、外商投资背景
B、为政务活动提供长期服务的能力
C、自主研发能力
D、境外认证机构合作资质
答案：B

38. 根据《商用密码管理条例》，申请商用密码进出口许可时无需提供（　）。
A、最终用户和用途证明
B、技术说明
C、申请人身份证明
D、密码源代码
答案：D

39. 依据《商用密码管理条例》，大众消费类密码产品（如手机加密芯片）在进出口时适用何种管理制度？（　）
A、需申请进口许可证
B、需通过国家安全审查
C、不实行进口许可和出口管制
D、仅需向海关报备
答案：C

40. 外商投资电子政务电子认证服务时，若影响国家安全，依据《商用密码管理条例》必须履行的程序是（ ）。
A、向密码管理部门备案
B、依法进行外商投资安全审查
C、取得国际认证资质
D、限制服务范围
答案：B

41. 关键信息基础设施运营者未按《商用密码管理条例》要求开展商用密码应用安全性评估，可能导致的最轻处罚是（ ）。
A、直接吊销运营资质
B、处 100 万元罚款
C、责令改正并给予警告
D、追究刑事责任
答案：C

42. 某企业销售未经检测认证的商用密码产品，违法所得 5 万元，根据《商用密码管理条例》，市场监管部门可并处多少罚款？（ ）
A、3 万元
B、10 万元
C、3 万元以上 10 万元以下
D、15 万元
答案：C

43. 电子政务电子认证服务机构因出具虚假认证结论被处罚，依据《商用密码管理条例》，可能面临的最高处罚是（ ）。
A、10 万元罚款
B、没收违法所得
C、吊销认证机构资质
D、追究法人刑事责任
答案：C

44. 某检测机构拟申请商用密码检测资质，依据《商用密码管理条例》，下列哪项是其必须具备的条件？（ ）
A、外资持股比例不超过 30%
B、具有法人资格和匹配的专业能力
C、获得网络安全等级保护认证
D、在境外设有分支机构
答案：B

45. 根据《中华人民共和国密码法》，商用密码领域的行业协会的功能和作用不包括（ ）。
A、为商用密码从业单位提供信息、技术、培训等服务
B、引导和督促商用密码从业单位依法开展商用密码活动
C、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
D、对商用密码从业单位开展收费检测认证

答案：D

46. 《商用密码管理条例》明确规定，制定条例的首要目的是规范商用密码应用和管理，同时还需兼顾哪项核心任务？（　）
A. 促进数字经济国际化
B. 鼓励和促进商用密码产业发展
C. 统一全国密码技术标准
D. 限制外资进入密码领域
答案：B

47. 密码管理部门依法开展监督检查时，依据《商用密码管理条例》，可行使的职权不包括（　）。
A、进入活动场所现场检查
B、复制合同账簿等资料
C、查封企业银行账户
D、调查法定代表人
答案：C

48. 根据《中华人民共和国密码法》，商用密码标准体系不包括（　）。
A、国家标准
B、团体标准
C、个人标准
D、行业标准
答案：C

49. 根据《中华人民共和国密码法》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（　）。
A、由密码管理部门进行
B、由市场监督管理部门进行
C、由市场监督管理部门会同密码管理部门进行
D、由市场监督管理部门或者密码管理部门进行
答案：C

50. 《商用密码管理条例》修订的考虑因素不包括（　　）
A、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
B、2019 年发布的《中华人民共和国密码法》对商用密码管理制度进行了结构性重塑
C、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
D、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
答案：C

二、多选题 15

1. 涉及国家安全的商用密码产品，依据《商用密码管理条例》，在销售前必须

完成哪些程序？（ ）
A、列入网络关键设备目录
B、经检测认证合格
C、取得发明专利
D、通过外商投资审查
答案：AB

2. 根据《中华人民共和国密码法》，以下属于商用密码从业单位的有（ ）。
A、某外商投资商用密码研发企业
B、某国有商用密码生产企业
C、某自然人控股的商用密码服务企业
D、某混合所有制的商用密码销售企业
答案：ABCD

3. 我国积极推动参与商用密码国际标准化活动，根据《中华人民共和国密码法》，以下可以参与制定商用密码国际标准的主体有（ ）。
A、企业
B、社会团体
C、教育机构
D、科研机构
答案：ABCD

4. 商用密码检测机构出现下列哪些情形，依据《商用密码管理条例》可能被吊销资质？（ ）
A、超出批准范围检测
B、检测数据虚假
C、未参与国际标准制定
D、拒不报送实施情况
答案：AB

5. 根据《中华人民共和国密码法》，关于商用密码行业协会的说法，正确的是（ ）。
A、目前很多省（自治区、直辖市）已经设立了商用密码行业协会
B、行业协会需经民政部门登记成立，否则属于非法组织
C、商用密码行业协会有助于实现密码行业的规范、健康发展
D、企业可以自愿申请加入行业协会
答案：ABCD

6. 以下关于《中华人民共和国密码法》的说法正确的有（ ）。
A、《中华人民共和国密码法》规范的是密码应用和管理
B、密码工作应坚持总体国家安全观
C、密码工作坚持中国共产党的领导
D、国家密码管理部门负责管理密码工作
答案：ABCD

7. 根据《中华人民共和国密码法》，密码工作应坚持的原则包括（ ）。

A、依法管理
B、统一负责
C、服务大局
D、创新发展
答案：ACD

8. 根据《中华人民共和国密码法》，下列关于我国密码工作管理体制的表述，正确的有（ ）。
A、国家密码管理部门负责管理全国的密码工作
B、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
C、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
D、密码工作保护部门负责本行业、本领域的密码工作
答案：ABC

9. 根据《中华人民共和国密码法》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（ ）。
A、推荐性国家标准
B、行业标准
C、团体标准
D、企业标准
答案：AB

10. 根据《中华人民共和国密码法》，我国商用密码出口管制的适用对象包括（ ）。
A、涉及国家安全的
B、涉及社会公共利益的
C、涉及大众消费的
D、涉及中国承担国际义务的
答案：ABD

11. 根据《中华人民共和国密码法》，以下符合商用密码的非歧视原则的做法包括（ ）。
A、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
B、基于自愿原则和商业规则开展商用密码技术合作
C、不得利用行政手段强制转让商用密码技术
D、利用行政手段强制转让商用密码技术
答案：ABC

12. 根据《中华人民共和国密码法》，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（ ）。
A、应按照法律法规和规定使用核心密码、普通密码
B、必要时可以使用商用密码进行临时传递和存储
C、使用 AES 256 进行加密保护
D、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

答案：BCD

13. 根据《中华人民共和国密码法》，（ ）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。
A、国家保密部门
B、密码管理部门
C、国家市场监督管理部门
D、国家民政部门
答案：ACD

14. 国家采取多种形式加强密码安全教育，根据《中华人民共和国密码法》，以下包括密码安全教育内容的教育体系有（ ）。
A、义务教育
B、公务员教育培训
C、高等教育
D、职业教育
答案：ABCD

15. 《中华人民共和国密码法》作为我国首部系统性规范密码工作的专门法律，既为国家安全构筑“技术盾牌”，又为数字经济发展注入法治动能。以下关于密码分类及管理要求的表述中，正确的有（ ）。
A、大众消费类产品采用的商用密码不实行进口许可和出口管制制度
B、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、社会公共利益或他人合法权益
C、县级以上地方密码管理部门负责管理本行政区域的核心密码和普通密码，国家密码管理部门统一管理商用密码
D、关键信息基础设施的运营者应委托第三方机构开展商用密码应用安全性评估
答案：AB

三、判断题 15
1、依据《中华人民共和国密码法》，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。
答案：错

2、依据《中华人民共和国密码法》，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。
答案：对

3、依据《中华人民共和国密码法》，公民、法人和其他组织可以依法使用普通密码保护网络与信息安全。
答案：错

4、发生核心密码、普通密码泄密案件的，依据《中华人民共和国密码法》，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。

答案：对

5、依据《中华人民共和国密码法》，密码管理部门可强制要求商用密码从业单位披露源代码。
答案：错

6、公安机关因反恐侦查需要，要求密码从业单位提供某商用社交软件的加密通信源代码，从业单位必须配合提供。
答案：错

7、依据《中华人民共和国密码法》，电子政务电子认证服务机构可无需国家密码管理部门认定即可开展服务。
答案：错

8、某企业向东南亚出口商用密码服务器，因未列入出口管制清单，未向商务部门申报直接通关，此操作合法。
答案：错

9、某政务系统存储机密级国家秘密信息，运维单位使用通过商用密码认证的加密产品进行保护，该行为符合《中华人民共和国密码法》要求。
答案：错

10、某市医院采购商用密码系统保护患者健康数据，因不属于关键信息基础设施，运营者可自行决定是否开展密码应用安全性评估。
答案：对

11、依据《商用密码管理条例》，商用密码团体标准的制定完全由市场自主决定，政府部门无需干预。
答案：错

12、依据《商用密码管理条例》，关键信息基础设施的商用密码保障系统可与主体工程分期建设。
答案：错

13、《商用密码管理条例》要求商用密码检测机构需向国家密码管理部门报送检测实施情况。
答案：对

14、依据《商用密码管理条例》，行政机关可基于行政管理需要，强制企业转让商用密码技术。
答案：错

15、依据《商用密码管理条例》，密码管理部门有权要求商用密码企业披露源代码以进行安全审查。
答案：错

二、网络安全法律法规 60

一、单选题 40

1. 下列哪一部法律给出了网络、网络安全、网络数据等用语的定义，并明确了部门、企业、社会组织和个人在网络空间中的权利、义务和责任？（　　）

A、《中华人民共和国网络安全法》
B、《中华人民共和国数据安全法》
C、《中华人民共和国个人信息保护法》
D、《中华人民共和国国家安全法》
答案：A

2. 《中华人民共和国网络安全法》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。

A、所有数据
B、一般数据
C、重要数据
D、网络日志
答案：C

3. 按照《中华人民共和国网络安全法》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。

A、自行
B、自行或者委托网络安全服务机构
C、委托网络安全服务机构
D、自行并且委托网络安全服务机构
答案：B

4. 按照《中华人民共和国网络安全法》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。

A、每三个月至少一次
B、每半年至少进行一次
C、每年至少进行一次
D、每两年至少一次
答案：C

5. 下列描述中，不符合《中华人民共和国网络安全法》的是（　　）。

A、网络产品应当符合相关国家标准的强制性要求
B、网络运营者可根据业务需要自行决定网络日志的留存时间
C、网络运营者应当制定网络安全事件应急预案
D、网络运营者收集个人信息应遵循正当、必要的原则
答案：B

6. 各级人民政府及其有关部门应当组织开展经常性的网络安全宣传教育，并指导、督促有关单位做好（　　）宣传教育工作。

A、网络安全
B、数据安全

C、信息安全
D、体系安全
答案：A

7. 国家鼓励开发网络数据安全保护和利用技术，促进（　　）资源开放，推动技术创新和经济社会发展。
A、事业单位数据
B、国企数据
C、企业数据
D、公共数据
答案：D

8. 国家支持网络运营者之间在网络安全信息收集、分析、通报和应急处置等方面进行合作，提高网络运营者的（　）能力。
A、数据运营
B、体系建设
C、安全保障
D、安全服务
答案：C

9. 网信部门和有关部门在履行网络安全保护职责中获取的信息，只能用于维护（　）的需要，不得用于其他用途。
A、信息安全
B、数据安全
C、隐私安全
D、网络安全
答案：D

10. 《中华人民共和国网络安全法》是网络安全领域“依法治国”的（　），对保障我国网络安全有着重大意义。
A、重要体现
B、唯一体现
C、重要指南
D、唯一指南
答案：A

11. 《中华人民共和国网络安全法》规定网络运营者应当对其收集的用户信息严格保密，并建立健全（　　）。
A、用户信息保密制度
B、用户信息保护制度
C、用户信息加密制度
D、用户信息保全制度
答案：B

12. 依据《中华人民共和国网络安全法》，国家积极开展网络空间治理、网络技术研发和标准制定、打击网络违法犯罪等方面的国际交流与合作，推动构建和平、

安全、开放、（ ）的网络空间。
A、多边
B、民主
C、透明
D、合作
答案：D

13. 某科技信息公司存有大量个人信息，根据《中华人民共和国个人信息保护法》要求，该公司应采取的保护措施，下列说法正确的是（ ）。
A、制定内部管理制度
B、定期对从业人员进行安全教育和培训
C、采取相应的加密、去标识化等措施
D、以上都是
答案：D

14. 按照《中华人民共和国个人信息保护法》，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（ ）。
A、因其认错态度较好且及时改正，公安机关仅对其进行警告
B、当地网信部门对其直接责任人员处以二百万元罚款
C、所属省级公安机关对其进行一千万元的罚款
D、当地网信部门对其进行三千万元的罚款
答案：C

15. 依据《中华人民共和国个人信息保护法》，（ ）是一旦泄露或者非法使用，容易导致自然人的人格尊严受到侵害或者人身、财产安全受到危害的个人信息，包括生物识别、宗教信仰、特定身份、医疗健康、金融账户、行踪轨迹等信息。
A、敏感个人信息
B、个人信息
C、个人数据
D、个人隐私
答案：A

16. 依据《中华人民共和国个人信息保护法》，提供重要互联网平台服务、用户数量巨大、业务类型复杂的个人信息处理者，应当定期发布（ ），接受社会监督。
A、个人信息风险评估报告
B、个人信息保护社会责任报告
C、个人信息保护影响评估报告
D、个人信息处理报告
答案：B

17. 根据《中华人民共和国个人信息保护法》，个人信息处理者在（ ）时不需要事前进行个人信息保护影响评估并对处理情况进行记录

A、利用匿名化的个人信息进行数据统计
B、处理敏感个人信息
C、向境外提供个人信息
D、进行对个人权益有重大影响的个人信息处理活动
答案：A

18. 《中华人民共和国个人信息保护法》立法宗旨不包括（　）。
A、为了保护个人信息权益
B、规范个人信息处理活动
C、提高个人信息数据质量
D、促进个人信息合理利用
答案：C

19. 个人信息处理者应当公开个人信息保护负责人的（　），并将个人信息保护负责人的姓名、联系方式等报送履行个人信息保护职责的部门。
A、身份证号
B、联系方式
C、家庭住址
D、工作地点
答案：B

20. 依据《中华人民共和国个人信息保护法》，国家机关处理的个人信息应当在中华人民共和国境内存储；确需向境外提供的，应当进行（　）。
A. 去标识化处理
B. 数据分类
C. 匿名化处理
D. 安全评估
答案：D

21. 依据《中华人民共和国个人信息保护法》，收集个人信息，应当限于实现处理目的的（　），不得过度收集个人信息。
A. 最小范围
B. 适中范围
C. 最大范围
D. 平均范围
答案：A

22. 《中华人民共和国个人信息保护法》的出台是我国个人信息保护立法史的重要里程碑，该法规定：提供（　　）、用户数量巨大、业务类型复杂的个人信息处理者，应建立健全个人信息保护合规制度体系。
A. 重要互联网平台服务
B. 基础性互联网平台服务
C. 关键信息基础设施
D. 基础设施服务平台
答案：A

23. 某在线教育平台计划收集 14 岁以下未成年人学习数据，并与境外机构共享以优化算法。隐私政策未明确境外接收方信息，仅通过默认勾选获取家长同意。根据《中华人民共和国个人信息保护法》，以下哪项是该平台必须补充或修正的关键措施？（ ）
A、删除所有儿童个人信息，改用匿名化数据替代
B、取得家长的单独书面同意，制定专门处理规则，并通过安全评估后向境外提供数据
C、仅需在隐私政策中增加“可能向境外传输数据”的提示即可
D、取消境外数据共享，改为境内存储以规避法律风险
答案：B

24. 《中华人民共和国数据安全法》旨在规范数据处理活动，保障数据安全，保护个人、组织的合法权益，维护国家主权、安全和发展利益。关于数据安全法，以下说法错误的是（ ）。
A、延续了网络安全法生效以来的“一轴两翼三级”的监管体系
B、是数据安全领域最高位阶的专门法
C、适用于在中国境内开展的数据处理活动及其安全监管
D、要求对不同类型和级别的数据采取相应的保护措施
答案：A

25. 按照《中华人民共和国数据安全法》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（ ）。
A、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
B、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
C、某关键信息基础设施运营者使用核心密码保护重要数据
D、某银行的重要数据使用核心密码进行加密保护
答案：A

26. 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《中华人民共和国数据安全法》，可对其实施的处置及处罚措施不包括（ ）。
A、当地公安机关责令其限期整改
B、当地公安机关对其给予警告的处罚
C、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
D、当地公安机关对其处以三十万元罚款
答案：C

27. 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《中华人民共和国数据安全法》的内容，对此下列说法正确的是（ ）。
D、有关主管部门有权对其进行警告
B、有关主管部门有权责令其整改
C、有关主管部门有权对其处以罚款
D、有关主管部门对直接负责的主管人员依法给予处分
答案：D

28. 根据《中华人民共和国数据安全法》，各地区、各部门应当按照数据（　　）制度，确定本地区、本部门以及相关行业、领域的重要数据具体目录，对列入目录的数据进行重点保护。
A、谁收集谁负责
B、安全监管协调
C、分类分级保护
D、谁公开谁负责
答案：C

29. 开展数据处理活动，应当遵守法律、法规，尊重社会公德和伦理，遵守商业道德和职业道德，诚实守信，履行数据安全保护义务，承担社会责任，不得危害国家安全、（　　），不得损害个人、组织的合法权益。
A、公共利益
B、国家利益
C、私有企业利益
D、国有企事业单位利益
答案： A

30. 国家促进数据安全（　　）等服务的发展，支持专业机构依法开展服务活动。
A、检测评估
B、检测认证
C、检测评估、认证
D、检测认证、备案
答案： C

31. 依据《中华人民共和国数据安全法》，（　）的处理者应当明确数据安全负责人和管理机构，落实数据安全保护责任。
A、个人信息
B、重要数据
C、敏感数据
D、机要数据
答案： B

32. 维护数据安全，应当坚持总体国家安全观，建立健全（　　），提高数据安全保障能力。
A、数据安全治理体系
B、数据安全保护体系
C、数据安全维护能力
D、数据安全治理能力
答案： A

33. 国家鼓励关键信息基础设施以外的（　　）自愿参与关键信息基础设施保护体系。
A、网络运营者
B、网络运维者
C、企事业单位

D、中高等院校
答案： A

34. 依据《中华人民共和国数据安全法》，各地区、各部门应当按照（ ），确定本地区、本部门以及相关行业、领域的重要数据具体目录，对列入目录的数据进行重点保护。
A. 数据安全管理制度
B. 数据安全审查制度
C. 网络安全等级保护制度
D. 数据分类分级保护制度
答案：D

35. 根据《中华人民共和国电子签名法》规定，从事电子认证服务，应当向（ ）提出申请。
A、国务院信息产业主管部门
B、国务院公安部门
C、国家密码管理部门
D、国家市场监督管理总局
答案：A

36. 根据《中华人民共和国电子签名法》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。
A、国务院商务主管部门
B、国家数据局
C、国家科技委员会
D、国家网信部门
答案：A

37. 在信息安全领域，我国出台了一系列的法律法规以保障国家网络安全和个人信息保护。以下关于这些法律法规的描述，哪一项是错误的？（ ）
A、《中华人民共和国个人信息保护法》于 2022 年 11 月 1 日起施行
B、《中华人民共和国数据安全法》于 2021 年 9 月 1 日起施行
C、《中华人民共和国网络安全法》于 2017 年 6 月 1 日起施行
D、《中华人民共和国密码法》于 2020 年 1 月 1 日起施行
答案：A

38. 按照《中华人民共和国个人信息保护法》，以下关于加密和去标识化的说法错误的是（ ）。
A、加密属于去标识化技术的一种
B、去标识化和加密属于不同的技术措施
C、去标识化可以和加密同时使用
D、对于敏感个人信息，去标识化后无必要再采用加密
答案：D

39. 《中华人民共和国电子签名法》规定，电子认证服务机构签发的证书内容失

实，造成损失时，应承担（　）。
A、仅需撤销证书
B、承担形式审查责任
C、证明无过错后可免责
D、一律承担连带赔偿责任
答案：C

40. 《中华人民共和国电子签名法》规定，满足法律要求的"电子文件原件"形式要件是（　）
A、首次生成时即加盖电子印章
B、内容未被系统自动备份
C、最终完整形成于专用系统
D、能够随时调取查用
答案：D

二、多选题 10

1.根据《中华人民共和国网络安全法》，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（　）。
A、确定网络安全负责人
B、采取防范网络攻击的技术措施
C、数据分类
D、重要数据备份
答案：ABCD

2.《中华人民共和国网络安全法》由全国人民代表大会常务委员会于 2016 年 11 月 7 日发布，下列关于此部法案说法错误的是（　）。
A、为了保障网络安全，维护网络空间主权和国家安全、社会公共利益，保护公民、法人和其他组织的合法权益，促进经济社会信息化健康发展，制定本法
B、确定了培养网络安全人才法律制度
C、采取监测、记录网络运行状态、网络安全事件的技术措施，并按照规定留存相关的网络日志不少于 360 天
D、《中华人民共和国网络安全法》自 2017 年 7 月 1 日起施行
答案：CD

3. 下列关于“网络信息安全”说法正确的有（　）。
A、网络运营者应当对其收集的用户信息严格保密
B、网络运营者无需建立用户信息保护制度
C、网络运营者不得泄露、篡改、毁损其收集的个人信息
D、在经过处理无法识别特定个人且不能复原的情况下，可以未经被收集者同意，网络运营者向他人提供个人信息
答案：AC

4. 根据《中华人民共和国电子签名法》，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（ ）。
A、涉及婚姻、收养、继承等人身关系的
B、涉及停止供水、供热、供气等公用事业服务的
C、涉及财产交易的民事合同
D、涉及房屋确权的单证文书
答案：AB

5. 按照《中华人民共和国个人信息保护法》，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（ ）。
A、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
B、通知应包括事件发生的原因和可能造成的后果
C、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
D、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
答案：ABCD

6. 根据《中华人民共和国电子签名法》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（ ）。
A、电子签名制作数据用于电子签名时，属于电子签名人专有
B、签署时电子签名制作数据仅由电子签名人控制
C、签署后对电子签名的任何改动能够被发现
D、签署后对数据电文内容和形式的任何改动能够被发现
答案：ABCD

7. 按照《中华人民共和国个人信息保护法》，在个人信息出境前，应考虑的安全保护机制有（ ）。
A、制定出境计划
B、开展出境评估
C、进行加密或采取去标识化措施
D、签订出境合同
答案：BCD

8. 《中华人民共和国个人信息保护法》中对提供重要互联网平台服务、用户数量巨大、业务类型复杂的个人信息处理者应履行的义务进行了要求。以下义务描述，正确的是（ ）。
A、 成立主要由内部成员组成的独立机构对个人信息保护情况进行监督
B、对严重违反法律、行政法规处理个人信息的平台内的产品或者服务提供者，停止提供服务
C、定期发布个人信息保护社会责任报告，接受社会监督
D、 遵循公开、公平、公正的原则，制定平台规则
答案：BCD

9. 某跨境电商企业收集用户消费记录（含住址、支付账户）后，未进行安全评估即通过标准合同将数据传输至境外服务器。因境外合作方安全漏洞，部分用户数据遭泄露，引发用户集体诉讼。根据《中华人民共和国个人信息保护法》，该企业的违法行为包括哪些？（ ）

A、未通过国家网信部门安全评估擅自跨境提供数据
B、未采取必要措施确保境外接收方达到保护标准
C、未向用户明示境外接收方信息并取得单独同意
D、未及时删除数据且拒绝用户行使删除权
答案：ABC

10. 国家积极开展数据安全治理、数据开发利用等领域的国际交流与合作，参与数据安全相关国际规则和标准的制定，下列说法错误的是（　）。
A、数据随意跨境，无需监管
B、数据跨境需要监管
C、为了商业利益，数据可以自由的交易而不需要审查
D、数据在交易之前应该接受审查
答案：AC

三、判断题 10
1. 《中华人民共和国网络安全法》规定，网信部门和有关部门在履行网络安全保护职责中获取的信息，只能用于维护网络安全的需要，不得用于其他用途。
答案：对

2. 根据《中华人民共和国网络安全法》，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。
答案：对

3. 《中华人民共和国网络安全法》是我国第一部全面规范网络安全的基础性法律。
答案：对

4. 任何个人和组织有权对危害网络安全的行为向网信、电信、公安等部门举报。收到举报的部门应当及时依法作出处理;不属于本部门职责的,也应当协调处理。
答案：错

5. 关键信息基础设施的运营者采购网络产品和服务，可能影响国家安全的，应当通过由国务院组织的国家安全审查。
答案：错

6. 依据《中华人民共和国个人信息保护法》，只有在具有特定的目的和充分的必要性,并采取严格保护措施的情形下,个人信息处理者方可处理敏感个人信息。
答案：对

7. 依据《中华人民共和国个人信息保护法》，国家监管机构负责统筹协调个人信息保护工作和相关监督管理工作。
答案：错

8. 《中华人民共和国个人信息保护法》规定，除法律、行政法规另有规定外，个人信息的保存期限应当为实现处理目的所预留的最充足时间。

答案：错

9. 在中华人民共和国境内建设、运营、维护、使用网络，以及网络安全的监督管理，适用《中华人民共和国网络安全法》。
答案：对

10. 《中华人民共和国数据安全法》所称数据，是指任何以电子或者其他方式对信息的记录。其中数据处理，包括数据的收集、存储、使用、加工、传输、提供、公开等。
答案：对

三、密码管理规章制度 60

一、单选题 40
1. 《网络安全审查办法》所称网络产品和服务不包括（　　）。
A、重要通信产品
B、云计算服务
C、核心网络设备
D、个人开发的软件
答案：D

2. 依据《网络安全审查办法》，网络安全审查办公室设在（　　），负责制定网络安全审查相关制度规范，组织网络安全审查。
A、国家互联网信息办公室
B、国家市场监督管理总局
C、工业和信息化部
D、国家网络安全和信息化委员会办公室
答案：A

3. 在（　　）的领导下建立了国家网络安全审查工作机制。
A、中央网络安全和信息化委员会
B、国家保密局
C、中国人民银行
D、国家市场监督管理总局
答案：A

4. 对于申报网络安全审查的采购活动，关键信息基础设施（　　）应当通过采购文件、协议等要求产品和服务（　　）配合网络安全审查。
A、运营者 提供者
B、提供者 运营者
C、组织者 运营者
D、提供者 使用者
答案：A

5. 网络安全审查中涉及的数据处理活动不包括数据的（　　）。

A、公开
B、存储
C、加工
D、售卖
答案：D

6. 网络平台运营者赴国外上市申报网络安全审查，可能的结果不包括（　　）。
A、无需审查
B、启动审查后，经研判不影响国家安全的，可继续赴国外上市程序
C、启动审查后，经研判影响国家安全的，不允许赴国外上市
D、启动审查后，经研判影响国家安全的，可继续赴国外上市程序
答案：D

7. 网络安全审查办公室认为需要开展网络安全审查的，如果情况复杂，可以延长（　　）个工作日。
A、15
B、30
C、60
D、90
答案：A

8. 根据《商用密码检测机构管理办法》规定，国家级商用密码检测机构的资质认定部门是（　　）。
A、省级密码管理部门
B、国家密码管理局
C、国务院市场监管总局
D、工业和信息化部
答案：B

9. 检测机构需变更法人代表的，按照《商用密码检测机构管理办法》中的要求，应（　　）。
A、自行变更后备案
B、提前 30 日申请审批
C、无需报备
D、事后 15 日内补交说明
答案：B

10. 若有检测机构超出指定范围开展检测的，依据《商用密码检测机构管理办法》规定，应受到的处罚是（　　）。
A、警告并限期整改
B、暂停资质 6 个月
C、吊销资质证书
D、处以违法所得 3 倍罚款
答案：C

11. 《商用密码检测机构管理办法》规定，检测机构资质延续申请应在有效期届

满前（　）提出。
A、30 日
B、60 日
C、90 日
D、180 日
答案：C

12. 若检测机构泄露商用密码技术秘密的，那检测机构最高可能承担（　）。
A、公开道歉
B、行政罚款
C、吊销资质
D、刑事责任
答案：D

13. 某银行规划新一代核心业务系统时，需依据《商用密码应用安全性评估管理办法》明确商用密码应用安全性评估的核心目标。该评估主要验证（　）。
A、密码产品价格合理性
B、密码应用的合规性、正确性及有效性
C、系统用户容量极限
D、硬件设备物理防护强度
答案：B

14. 省级医保信息系统被列为重要网络与信息系统，依据《商用密码应用安全性评估管理办法》，其商用密码评估工作的全国主管部门是（　）。
A、国家卫生健康委员会
B、国家密码管理局
C、省级人民政府
D、公安部网络安全保卫局
答案：B

15. 某电力调度系统运营者依据《商用密码应用安全性评估管理办法》建设密码保障系统时，必须遵守的原则是（　）。
A、先建设后补评估
B、与主体系统同步规划、建设、运行
C、每三年升级一次密码算法
D、仅委托第三方运维
答案：B

16. 某政务云平台规划阶段制定的商用密码应用方案未通过评估，依据《商用密码应用安全性评估管理办法》，应如何处理？（　）
A、可先依据建设再整改
B、不得作为密码系统建设依据
C、降低安全等级使用
D、向国家局申请特批
答案：B

17. 某电信运营商计费系统已运行 3 年，依据《商用密码应用安全性评估管理办法》，至少应多久开展一次商用密码应用安全性评估？（　）
A、每 6 个月
B、每年
C、每 18 个月
D、每 2 年
答案：B

18. 某能源集团完成评估报告后，依据《商用密码应用安全性评估管理办法》需在多长时间内向密码管理部门备案？（　）
A、15 个工作日
B、30 日内
C、下次评估前
D、90 个自然日
答案：B

19. 《商用密码应用安全性评估管理办法》生效前已运行的税务征管系统，应如何管理？（　）
A、豁免评估
B、每年开展评估
C、重新设计密码架构
D、仅做漏洞扫描
答案：B

20. 某国企自行开展商用密码应用安全性评估后，依据《商用密码应用安全性评估管理办法》，报告需由（　）签署生效。
A、外部审计师签字并加盖单位公章
B、密码或网络安全负责人签字并加盖单位公章
C、法务总监签字并加盖单位公章
D、IT 部门经理签字并加盖单位公章
答案：B

21. 关键信息基础设施运营者采购商用密码产品和服务，根据《关键信息基础设施商用密码使用管理规定》规定，应优先选择（　）。
A、自主创新产品
B、通过安全认证的产品
C、国际通用标准产品
D、价格最低的产品
答案：B

22. 根据《关键信息基础设施商用密码使用管理规定》规定，关键信息基础设施密码应用安全性评估的最低频率要求是（　）。
A、每年一次
B、每两年一次
C、上线前评估一次
D、发生重大变更时评估

答案：A

23. 根据《关键信息基础设施商用密码使用管理规定》规定，密码应用安全性评估报告应向哪个部门报送？（　）
A、公安机关
B、国家密码管理局
C、行业主管监管部门
D、网络安全等级保护机构
答案：C

24. 根据《关键信息基础设施商用密码使用管理规定》规定，关键信息基础设施密码保护的第一责任主体是（　）。
A、技术运维团队
B、运营单位主要负责人
C、密码服务提供商
D、行业监管部门
答案：B

25. 运营者委托第三方开展密码应用评估时，根据《关键信息基础设施商用密码使用管理规定》规定，受托方必须具备（　）。
A、网络安全等级保护资质
B、商用密码检测机构资质
C、ISO27001 认证
D、风险管理体系认证
答案：B

26. 根据《关键信息基础设施商用密码使用管理规定》规定，密码应用方案应包括的核心内容是（　）。
A、预算分配表
B、密码技术路线和实施计划
C、供应商名单
D、员工培训记录
答案：B

27. 发生密码安全事件后，根据《关键信息基础设施商用密码使用管理规定》规定，运营者向监管部门报告的最长时限是（　）。
A、1 小时
B、12 小时
C、24 小时
D、72 小时
答案：A

28. 密码应用安全性评估中，需重点保护的要素不包括（　）。
A、身份鉴别数据
B、操作日志
C、公开宣传材料

D、重要数据存储
答案：C

29. 运营者跨境提供重要数据时，根据《关键信息基础设施商用密码使用管理规定》规定，需依法开展的审查是（　）。
A、密码应用安全性评估
B、网络安全审查
C、个人信息影响评估
D、商业秘密审核
答案：B

30. 根据《关键信息基础设施商用密码使用管理规定》规定，在密码应用改造项目验收时，必须提交的材料是（　）。
A、用户满意度调查报告
B、密码应用安全性评估报告
C、供应商服务承诺书
D、项目决算审计报告
答案：B

31. 某市数据局需设立电子认证服务机构，依据《电子政务电子认证服务管理办法》，应取得哪个部门的资质认定？
A、工业和信息化部
B、国家密码管理局
C、公安部
D、市场监管总局
答案：B

32. 省级医保平台电子认证服务机构申请资质时，依据《电子政务电子认证服务管理办法》，无需满足哪项条件？（　）
A、30 名以上专业人员
B、外资控股股权结构
C、符合国标的认证系统
D、企业法人资格
答案：B

33. 电子签名认证证书失效后，依据《电子政务电子认证服务管理办法》，认证机构保存信息的法定最低年限是（　）。
A、3 年
B、5 年
C、10 年
D、永久
答案：B

34. 依据《电子政务电子认证服务管理办法》，电子政务电子认证服务机构拟暂停或者终止电子政务电子认证服务的，应当在暂停或者终止服务（　）向国家密码管理局报告。

A、30 日前
B、60 日前
C、90 日前
D、120 日前
答案：B

35. 某认证机构未公布投诉渠道，依据《电子政务电子认证服务管理办法》，可能面临的罚款金额是（ ）。
A、5 千-5 万元
B、1 万-10 万元
C、违法所得 1-3 倍
D、30 万元以上
答案：B

36. 认证机构发现服务器遭黑客入侵，依据《电子政务电子认证服务管理办法》，需在多少日内向省级密码部门报告？（ ）
A、立即报告
B、15 日
C、30 日
D、60 日
答案：B

37. 某省社保平台电子认证机构迁移核心系统，依据《电子政务电子认证服务管理办法》，需在变更后多少日内向国家密码管理局报告？（ ）
A、15 日
B、30 日
C、60 日
D、90 日
答案：B

38. 国家密码管理局委托技术评审时，依据《电子政务电子认证服务管理办法》，专家需对什么负责？（ ）
A、评审费用结算
B、结论真实性及符合性
C、申请人商业机密
D、行政许可决定
答案：B

39. 某认证机构将证书注册业务委托给 A 公司，A 公司又以自身名义委托 B 公司，依据《电子政务电子认证服务管理办法》，责任主体是（ ）。
A、A 公司
B、原认证机构
C、B 公司
D、三方共担
答案：B

40. 电子政务电子认证服务机构因泄露公民信息被查处，依据《电子政务电子认证服务管理办法》，可能面临的最重处罚是（　）。
A. 10 万元罚款
B. 停业整顿
C. 没收违法所得
D. 吊销资质
答案：D

二、多选题 10
1. 实施《网络安全审查办法》的理念包括（　）。
A、坚持防范网络安全风险与促进先进技术应用相结合
B、坚持过程公正透明与知识产权保护相结合
C、坚持事前审查与持续监管相结合
D、坚持企业承诺与社会监督相结合
答案：ABCD

2. 以下行为符合《网络安全审查办法》的是（　）。
A、不利用提供产品和服务的便利条件非法获取用户数据
B、不非法控制和操纵用户设备
C、不中断产品供应或者必要的技术支持服务
D、关键信息基础设施运营者采购网络产品和服务不主动申报网络安全审查
答案：ABC

3. 网络安全审查重点评估相关对象或者情形的国家安全风险因素包括（　）。
A、产品和服务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
B、产品和服务供应报价对关键信息基础设施业务运维成本的影响
C、产品和服务提供者遵守中国法律、行政法规、部门规章情况
D、核心数据、重要数据或者大量个人信息被窃取、泄露、毁损以及非法利用、非法出境的风险
答案：ACD

4. 关键信息基础设施运营者、网络平台运营者违反《网络安全审查办法》规定的，依照（　）的规定处理。
A、《中华人民共和国网络安全法》
B、《中华人民共和国数据安全法》
C、《网络安全审查办法》
D、《中华人民共和国密码法》
答案：AB

5. 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（　）。
A、申报书
B、采购文件或协议
C、关于影响或者可能影响国家安全的分析报告
D、网络安全审查工作需要的其他材料

答案：ABCD

6. 依据《商用密码检测机构管理办法》规定，检测机构在业务开展中须履行的义务包括（　）。
A、公开收费标准
B、建立保密制度
C、接受年度评估
D、公示检测流程
答案：ABCD

7. 依据《商用密码检测机构管理办法》规定，以下哪些情形将导致资质暂停？（　）
A、未通过年度评估
B、超范围检测
C、检测报告造假
D、变更地址未备案
答案：AC

8. 在《商用密码检测机构管理办法》中描述的，国家密码管理局对检测机构的监管手段包括（　）。
A、飞行检查
B、约谈负责人
C、公开通报批评
D、吊销资质证书
答案：ABCD

9. 根据《关键信息基础设施商用密码使用管理规定》规定，以下哪些情形必须重新开展密码应用安全性评估？（　）
A、系统架构重大变更
B、发现高风险漏洞
C、年度例行评估到期
D、更换密码服务商
答案：AB

10. 依据《电子政务电子认证服务管理办法》，密码管理部门依法对电子政务电子认证服务活动进行监督检查，其中监督检查可以采取的方式有（　）。
A、网络监测
B、实地核查
C、冻结银行账户
D、公开听证
答案：AB
三、判断题 10
1. 《商用密码检测机构管理办法》规定，检测机构可自愿申请成为国家级或区域性机构。（　）
答案：对

2. 《商用密码检测机构管理办法》规定，检测机构对委托方提供的技术资料负有永久保密义务。（　　）
答案：对

3. 《商用密码检测机构管理办法》提到区域性检测机构经批准可在其他省份设立分支机构。（　　）
答案：错

4. 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。（　　）
答案：错

5. 某市密码管理局对医保系统开展专项检查，依据《商用密码应用安全性评估管理办法》，属于合法职权范围。（　　）
答案：对

6. 某银行因未开展年度评估被罚 120 万元，依据《商用密码应用安全性评估管理办法》，超过罚款上限。（　　）
答案：对

7. 某支付平台评估未通过，依据《商用密码应用安全性评估管理办法》，改造期间可保持业务运行无需额外措施。（　　）
答案：错

8. 根据《关键信息基础设施商用密码使用管理规定》规定，密码应用安全性评估可由运营者内部技术团队自行开展。（　　）
答案：错

9. 依据《电子政务电子认证服务管理办法》，电子政务电子认证服务机构应当于每年 1 月 30 日前向住所地省、自治区、直辖市密码管理部门报送上一年度工作报告。（　　）
答案：错

10. 认证机构变更办公地址未报告，依据《电子政务电子认证服务管理办法》，需 30 日内办理变更手续。（　　）
答案：对

四、其他政策法规条例 50

一、单选题 30

1. 某省级单位新建政务信息系统，根据《江苏省省级政务信息化项目建设管理办法》规定，项目单位应如何落实密码应用要求？（　）
A、项目建成后补充密码保障方案
B、同步规划、建设、运行密码保障系统并定期评估
C、仅需在验收时提供密码技术说明
D、委托第三方机构代建密码系统

答案：B

2. 依据《江苏省省级政务信息化项目建设管理办法》，（　）负责项目安全可靠情况、密码应用、电子文件管理等审核及监督工作。
A、省国家密码管理局
B、省发展改革委
C、省保密局
D、省委网信办
答案：A

3. 依据《江苏省省级政务信息化项目建设管理办法》，密码应用安全性评估结果不合格的项目，将面临（　）。
A、扣减 50%运维经费
B、不得申请竣工验收
C、限期 3 个月整改
D、通报批评责任单位
答案：B

4. 依据《江苏省数据条例》，（　　）是数据安全责任主体，应建立健全数据安全管理制度，组织开展数据安全教育培训，采取相应的技术措施和其他必要措施，加强数据处理全流程安全防护。
A、数据提供者
B、数据收集者
C、数据使用者
D、数据处理者
答案：D

5. 《江苏省数据条例》自 2025 年 4 月 1 日起施行，旨在加强数据资源管理，保障数据安全，促进数据依法有序流通和应用，其中，规定（　　）按照国家有关规定统筹协调全省数据跨境流动安全管理工作。
A、省工业和信息化部门
B、省网信部门
C、省通信管理部门
D、省数据部门
答案：B

6. 《关键信息基础设施安全保护条例》在法律责任部分细化了在安全保护全过程中，各个环节违反相应条例的具体处罚措施。以下说法错误的是（　　）。
A、受到治安管理处罚的人员，5 年内不得从事网络安全管理和网络运营关键岗位的工作
B、受到刑事处罚的人员，10 年内不得从事网络安全管理和网络运营关键岗位的工作
C、违反条例规定，给他人造成损害的，依法承担民事责任
D、运营者未设置专门安全管理机构的，由有关主管部门依据职责责令改正，给予警告
答案：B

7. 《网络数据安全管理条例》规定，网络数据处理者向其他网络数据处理者提供、委托处理个人信息和重要数据的处理情况记录，应当至少保存（　　）。
A、1 年
B、2 年
C、3 年
D、5 年
答案：C

8. 依据《江苏省政务信息化项目建设网络安全管理规定》，运营单位应当建立技术服务外包（　　），及时评估服务外包的网络安全风险，在服务合同（协议）中明确网络安全责任和要求。
A、人员管理制度
B、风险管理制度
C、安全责任划分制度
D、网络安全管理制度
答案：D

9. 根据《江苏省政务信息化项目建设网络安全管理规定》实施指南，（　）会同省有关部门强化对省政务信息化项目的网络安全检查和评估，对于不符合网络安全要求，或者存在重大安全隐患的政务信息系统，发放《运行管理安全问题整改通知单》。
A、省委网信办
B、省工业和信息化厅
C、省政府办公厅
D、省国家密码管理局
答案：A

10. 根据我国积极促进数据依法有序自由流动，国家互联网信息办公室结合数据出境安全管理工作实际，制定了《促进和规范数据跨境流动规定》，规定了通过数据出境安全评估结果有效期为（　　），自评估结果出具之日起计算。
A、1 年
B、2 年
C、3 年
D、4 年
答案：C

11. 为了规范个人信息保护合规审计活动，根据《中华人民共和国个人信息保护法》、《网络数据安全管理条例》等法律、法规，制定了《个人信息保护合规审计管理办法》，该办法自（　　）起施行。
A、2025 年 3 月 1 日
B、2025 年 4 月 1 日
C、2025 年 5 月 1 日
D、2025 年 6 月 1 日
答案：C

12. 隐私保护技术是针对个人信息安全保护的重要措施，常见的隐私保护技术有泛化、抑制、置换、裁剪、扰动等。若只显示前几位数字而不显示完整的电话号码，属于（　　）。
A、置换
B、裁剪
C、抑制
D、泛化
答案：B

13. 商用密码日近年来，国际国内形势发生深刻变化，保密工作面临着新形势新任务，为进一步健全保密管理体制机制，完善保密管理制度，我国颁布了《中华人民共和国保守国家秘密法》，其正式施行日期为（　　）。
A、2024 年 3 月 1 日
B、2024 年 4 月 1 日
C、2024 年 5 月 1 日
D、2024 年 6 月 1 日
答案：C

14. 依据《互联网政务应用安全管理规定》，机关事业单位应当自行或者委托具有相应资质的第三方网络安全服务机构，对互联网政务应用网络和数据安全（　　）至少进行一次安全检测评估。
A、每半年
B、每年
C、每两年
D、每三年
答案：B

15. 关于信息安全保障的概念，下面说法错误的是（　　）。
A、信息系统面临的风险和威胁是动态变化的，信息安全保障强调动态的安全理念
B、信息安全保障已从单纯保护和防御阶段发展为集保护、检测和响应为一体的综合阶段
C、在全球互联互通的网络空间环境下，可单纯依靠技术措施来保障信息安全
D、信息安全保障把信息安全从技术扩展到管理，通过技术、管理和工程等措施的综合融合，形成对信息、信息系统 及业务使命的保障
答案：C

16. 以下哪一项不是我国国务院信息化办公室为加强信息安全保障明确提出的九项重点工作内容之一（　　）
A、提高信息技术产品的国产化率
B、保证信息安全资金投入
C、加快信息安全人才培养
D、重视信息安全应急处理工作
答案：A

17. 密码工作坚持（　　）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。
A、国家大局
B、统筹国家
C、总体国家
D、国家全局
答案：C

18. 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。
A、国家互联网信息办公室
B、海关总署
C、国家密码管理局
D、国家数据局
答案：C

19. 根据《关键信息基础设施安全保护条例》，关键信息基础设施发生重大网络安全事件或者发现重大网络安全威胁时，运营者应当按照有关规定向保护工作部门、（　　）报告。
A、网信部门
B、网安部门
C、公安机关
D、电信部门
答案：C

20. 《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。
A、公民、法人和其他组织的合法权益
B、社会秩序
C、公共利益
D、国家安全
答案：D

21. 关于商用密码应用安全性评估的原则，以下表述错误的是（　）。
A、商用密码应用安全性评估实施分类分级管理
B、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
C、已建成的重要领域网络和信息系统不再需要开展评估
D、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
答案：C

22. 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（　）。
A、机密性、真实性、完整性、不可否认性
B、秘密性、确定性、完整性、不可替代性

C、机密性、安全性、统一性、不可抵赖性
D、秘密性、有效性、统一性、不可逆转性
答案：A

23. 依据《互联网信息服务管理办法》，互联网信息服务提供者应当向上网用户提供良好的服务，并保证所提供的（　）。
A、信息内容合法
B、信息内容有效
C、信息内容规范
D、信息内容及时
答案：A

24. 《江苏省公共数据管理办法》规定：（　）会同有关主管部门建立公共数据管理安全应急处置机制，指导公共管理和服务机构制定安全处置应急预案，定期组织应急演练。
A、工信部门
B、网信部门
C、电信部门
D、数据管理部门
答案：B

25. 《App 违法违规收集使用个人信息行为认定方法》系《中华人民共和国网络安全法》框架下针对广泛应用的 App 的个人信息保护配套性规章。下列（　）可以被认定为“违反必要原则，收集与其提供的服务无关的个人信息”？
A. 一款天气预报 App 仅收集用户的位置信息用于提供本地天气预报
B. 一款社交媒体 App 收集用户位置信息用于向用户推荐附近的活动
C. 一款健康管理 App 收集用户的健康数据用于提供健康建议
D. 一款游戏 App 收集用户的银行账户信息，声称是为防止作弊行为
答案：D

26. 随着数字化进程的加快，公共数据的安全问题日益突出。依据《江苏省公共数据管理办法》，公共数据提供按照（　）的原则，实施公共数据管理。
A、谁主管谁负责、谁提供谁负责
B、谁主管谁负责、谁使用谁负责
C、谁管理谁负责、谁使用谁负责
D、谁使用谁负责、谁提供谁负责
答案：A

27. 依据《江苏省公共数据管理办法》，公共管理和服务机构之间共享公共数据应当以（　）为原则、（　）为例外，（　）公共数据。
A、不共享、共享、无偿共享
B、不共享、共享、有偿共享
C、共享、不共享、有偿共享
D、共享、不共享、无偿共享
答案：D

28. 依据《江苏省省级政务信息化项目建设管理办法》，项目单位在哪个阶段需首次制定密码应用方案？（　）
A、项目建成阶段
B、项目实施阶段
C、竣工验收阶段
D、运维阶段
答案：B

29. 依据《区块链信息服务管理规定》，区块链信息服务提供者应当记录区块链信息服务使用者发布内容和日志等信息，记录备份应当保存不少于（　），并在相关执法部门依法查询时予以提供。
A、一个月
B、三个月
C、六个月
D、九个月
答案：C

30. 当前，个人信息被企业、机构甚至个人广泛收集使用，个人信息保护和个人信息利用的矛盾日益突出。那么，根据《个人信息保护合规审计管理办法》要求，如果某大型电商平台处理超过 1500 万用户个人信息，该平台合规审计的最低频率应为（　）。
A、每半年一次
B、每年一次
C、每两年一次
D、每三年一次
答案：C

二、多选题 10
1. 依据《网络数据安全管理条例》，重要数据的处理者应当每年度对其网络数据处理活动开展风险评估，并向省级以上有关主管部门报送风险评估报告，有关主管部门应当及时通报同级（　）。
A、网信部门
B、公安机关
C、保密行政管理部门
D、工业和信息化部门
答案：AB

2. 关键信息基础设施是国家安全的核心命脉，涉及能源、交通、金融、国防等关键领域。请结合《关键信息基础设施安全保护条例》内容，将责任主体与对应的法定职责或权限正确连线：

责任主体	法定职责
1. 国家网信部门	A. 制定本行业、本领域关键信息基础设施认定规则
2. 保护工作部门	B. 统筹协调跨部门网络安全信息共享与威胁研判
3. 运营者	C. 对专门安全管理机构负责人实施安全背景审查

责任主体　　法定职责

4. 公安机关　　D. 依法指导监督全国关键信息基础设施安全保护

A、1—B；2—A；3—C；4—D
B、1—A；2—C；3—D；4—B
C、1—C；2—D；3—B；4—A
D、1—D；2—B；3—A；4—C
答案：A

3. 依据工业互联网数据的重要性以及在发生安全事件时可能造成的影响范围与程度不同，划分为低重要性、中重要性及高重要性数据。结合《工业互联网数据安全保护要求》，以下属于高重要性数据的是（　　）。
A、 生产控制数据
B、生产管理数据
C、设备日志数据
D、 环境数据
答案：AB

4. 《中华人民共和国民法典》被称为“社会生活的百科全书”，是一个国家经济社会发展的真实写照。以下有关《中华人民共和国民法典》的说法，正确的是（　　）。
A、首次明确了隐私的定义
B、规定了处理个人信息应遵循的原则和条件
C、规定了处理个人信息的免责情形
D、规定了信息处理者的信息安全保障义务
答案：ABCD

5. 我国《中华人民共和国刑法》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（　）。
A、走私国家禁止进出口的货物、物品罪
B、非法经营罪
C、泄露国家秘密罪
D、逃避商检罪
答案：AD

6. 去标识化不仅仅是对数据集中的直接标识符、准标识符进行删除和变换，也可以结合后期应用场景考虑数据集被重标识的风险。依据《个人信息去标识化指南》，建立去标识化目标，需要考虑的因素有（　　）。
A、 数据用途
B、数据来源
C、风险级别
D、 去标识化模型
答案：ABCD

7. 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（　）
A、商用密码产品认证证书的有效期为五年

B、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
C、认证证书覆盖产品变更的，认证证书有效期不变
D、认证证书覆盖产品扩展的，认证证书有效期自动终止
答案：ABC

8. 关于《电子认证服务使用密码许可证》，下列说法正确的是（　）。
A、有效期为 5 年
B、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
C、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》
D、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》
答案：ABD

9. 《江苏省数据条例》已由江苏省第十四届人民代表大会第三次会议于 2025 年 1 月 22 日通过，自 2025 年 4 月 1 日起施行。那么，请将以下数据应用领域与其对应的条例内容进行正确匹配：

应用领域	条例内容
1. 制造业领域的数据应用	A. 推动智能车间、智能工厂建设，构建制造业基础数据库
2. 农业领域的数据应用	B. 制定自贸区数据出境清单，探索一般数据自由流动
3. 公共服务领域的数据应用	C. 整合医疗、教育等数据资源，推进城市全域数字化转型
4. 数据跨境流通试点	D. 建设农业生产数智化场景，提升数字化精准管理水平

A、1—A；2—D；3—C；4—B
B、1—D；2—B；3—A；4—C
C、1—B；2—C；3—D；4—A
D、1—C；2—A；3—B；4—D
答案：A

10. 江苏省省级政务信息化项目申请竣工验收时，依据《江苏省省级政务信息化项目建设管理办法》，需同步提交哪些关键材料？（　）
A、项目建设总结
B、财务审计报告
C、安全风险评估报告
D、密码应用安全性评估报告
答案：ABCD

三、判断题 10
1. 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。
答案：对

2. 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《中华人民共和国密码法》等相关法律、行政法规的规定。
答案：对

3. 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。
答案：对

4. 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。
答案：错

5. 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。
答案：错

6. 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。
答案：对

7. 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《中华人民共和国认证认可条例》做出决定，无需征求国家密码管理部门的意见。
答案：错

8. 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。
答案：对

9. 省级政务信息化项目建成后 6 个月内，依据《江苏省省级政务信息化项目建设管理办法》，项目单位提交验收申请报告时可暂不含密码应用安全性评估报告。
答案：错

10. 《商用密码应用安全性评估管理办法》规定，重要网络与信息系统建成运行后，其运营者应当自行或者委托商用密码检测机构每两年至少开展一次商用密码应用安全性评估，确保商用密码保障系统正确有效运行。
答案：错

第二部分专业题 800

一、密码学 400

一、单选题 162

1. 数字签名（又称公钥数字签名、电子签章）是一种类似写在纸上的普通的物理签名，是非对称密钥加密技术与数字摘要技术的应用。数字签名主要是解决信息的（　　）。

A、完整性
B、机密性
C、不可否认性
D、可认证性
答案：C

2. 为实现消息的不可否认性，A 发送给 B 的消息需使用（　　）进行数字签名。

A、A 的公钥
B、A 的私钥
C、B 的公钥
D、B 的私钥
答案：B

3. 密码学理论研究通常包括哪两个分支（　　）。

A、对称加密与非对称加密
B、密码编码学与密码分析学
C、序列算法与分组算法
D、DES 和 RSA
答案：B

4. 以下选项中各种加密算法中属于非对称加密算法的是（　　）。

A、DES 算法
B、Caesar 密码
C、Vigenere 密码
D、RSA 算法
答案：D

5. 对 RSA 算法的描述正确的是（　　）。

A、RSA 算法是对称密钥算法
B、RSA 算法是公钥算法
C、RSA 算法是一种流密码
D、RSA 算法是杂凑函数算法
答案：B

6. 杂凑函数不可直接应用于（　　）。

A、数字签名
B、安全存储口令
C、加解密

D、数字指纹
答案：C

7. 以下不是 SM2 算法的应用场景的有（　　）。
A、生成随机数
B、协商密钥
C、加密数据
D、数字签名
答案：A

8. 一个序列密码具有很高的安全强度主要取决于（　　）。
A、密钥流生成器的设计
B、初始向量长度
C、明文长度
D、加密算法
答案：A

9. 以下哪不属于密码学的具体应用的是（　　）。
A、人脸识别技术
B、消息认证，确保信息完整性
C、加密技术，保护传输信息
D、进行身份认证
答案：A

10. （　　）原则上能保证只有发送方与接收方能访问消息内容。
A、保密性
B、鉴别
C、完整性
D、数字签名
答案：A

11. 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（　　）。
A、同步序列密码
B、非同步序列密码
C、自同步序列密码
D、移位序列密码
答案：A

12. （　　）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。
A、对称
B、私钥
C、代换
D、公钥
答案：D

13. 下列选项中不属于公钥密码体制的是（　　）。
A、ECC
B、RSA
C、ELGamal
D、DES
答案：D

14. 原始的 Diffie-Hellman 密钥交换协议易受（　　）。
A、中间人攻击
B、选择密文攻击
C、已知明文攻击
D、被动攻击
答案：A

15. 多变量公钥密码的安全性基础是基于（　　）的困难性。
A、求解有限域上随机生成的多变量非线性多项式方程组
B、大整数分解
C、任意线性码的译码问题
D、最小整数解问题
答案：A

16. 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（　　）。
A、计算上安全
B、不安全
C、无条件安全
D、不可破译
答案：A

17. 数字签名能够提供，而消息认证码无法提供的安全属性是（　　）。
A、机密性
B、认证
C、随机性
D、不可否认性
答案：D

18. 下列选项不是密码系统基本部分组成的是（　　）。
A、明文空间
B、密码算法
C、初始化
D、密钥
答案：C

19. 关于对称加密和非对称加密，以下说法正确的是（　　）。
A、对称加密的安全性较高
B、对称加密一定比非对称加密的安全性高

C、对称加密的效率较高
D、非对称加密的效率较高
答案：C

20. 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。
A、3
B、4
C、5
D、32
答案：A

21. 下述哪些变换（　　）与 SM4 算法的安全强度无关。
A、S 盒变换
B、线性变换
C、轮密钥异或加变换
D、反序变换
答案：D

22. 下列关于 SM4 分组密码算法叙述错误的是（　　）。
A、一般来说，分组密码迭代轮数越多，密码分析越困难
B、可以用于数据加密
C、是对称密码
D、是不可逆的
答案：D

23. 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(　　)。
A、都是 8 比特输入 8 比特输出的非线性置换
B、都是基于有限域逆运算构造
C、两者之间线性等价
D、两者之间仿射等价
答案：C

24. 下列关于 SM4 分组密码算法叙述正确的是（　　）。
A、一次只对明文消息的单个字符进行加解密变换
B、是不可逆的
C、采用了正形置换设计思想
D、需要密钥同步
答案：C

25. 下列关于 SM4 的解密算法叙述错误的是（　　）。
A、解密算法与加密算法结构相同
B、解密轮密钥与加密轮密钥相同
C、解密轮密钥是加密轮密钥的逆序
D、解密算法与加密算法都采用 32 轮迭代
答案：B

26. 下列关于 SM4 的密钥扩展算法叙述错误的是（　　）。
A、采用 32 轮非线性迭代结构
B、每次迭代生成 32 比特轮密钥
C、采用与加密算法相同的 S 盒
D、采用与加密算法相同的线性变换
答案：D

27. SM4 加密算法的线性变换 L 存在（　　）个固定点。
A、0
B、1
C、2
D、4
答案：D

28. 序列密码也称为（　　），它是对称密码算法的一种。
A、非对称密码
B、公钥密码
C、流密码
D、古典密码
答案：C

29. 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。
A、对称
B、非对称
C、古典
D、一次一密
答案：D

30. 以下是序列密码或流密码算法的是（　　）。
A、SM2 算法
B、SM3 算法
C、SM4 算法
D、ZUC 算法
答案：D

31. m 序列是（　　）移位寄存器序列的简称。
A、最长线性
B、最短线性
C、最长非线性
D、最短非线性
答案：A

32. 关于椭圆曲线密码体制正确的是（　）。
A、运算速度一般比对称密码算法快

B、运算速度一般与对称密码一样快
C、密钥长度一般比同等强度的 RSA 短
D、密钥长度一般比同等强度的 RSA 长
答案：C

33. 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。
A、3G
B、4G
C、5G
D、2G
答案：C

34. 关于杂凑函数下列描述有错误的是（　　）。
A、杂凑函数的输入长度固定
B、杂凑 123.函数的输出长度固定
C、杂凑函数可用于数字签名方案
D、杂凑函数可用于消息完整性机制
答案：A

35. 下面（　　）不是杂凑函数的主要应用。
A、文件完整性验证
B、数字签名
C、数据加密
D、身份鉴别协议
答案：C

36. SHA-1 接收任何长度的输入消息，并产生长度为（　　）位的杂凑值。
A、64
B、160
C、512
D、128
答案：B

37. 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（　　）。
A、2^16
B、2^32
C、2^48
D、2^64
答案：B

38. 对于一个给定的杂凑函数 H，其单向性是指（　　）。
A、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
B、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
C、找到任何满足 H(x)=H(y)的(x，y)在计算上是不可行的
D、以上说法都不对
答案：A

39. MD5 算法输出报文杂凑值的长度为（　　）。
A、120
B、128
C、144
D、160
答案：B

40. SM3 是（　　）算法。
A、分组密码
B、公钥密码
C、数字签名
D、密码杂凑函数
答案：D

41. SM3 密码杂凑算法的链接变量长度为（　　）比特。
A、128
B、224
C、256
D、512
答案：C

42. 在公钥密码体制中，加密过程中用（　　）。
A、对方的公钥
B、自己的公钥
C、自己的私钥
D、用公钥和私钥
答案：A

43. RSA 公钥密码算法的安全性基于（　　）。
A、模指数计算
B、离散对数求解问题
C、数论中大整数分解的困难性
D、Euler 定理
答案：C

44. ElGamal 公钥密码体制的安全性基于（　　）。
A、数域上的离散对数问题
B、椭圆曲线上的离散对数问题
C、数域上大整数素数分解问题
D、椭圆曲线上大整数素数分解问题
答案：A

45. 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(　　)。
A、不同
B、相同

C、有时相同，也有不同
D、根据具体情况
答案：A

46. 利用 SM2 公钥密码体制两次加密相同的明文，密文（　　）。
A、不同
B、相同
C、有时相同，也有不同
D、根据具体情况
答案：A

47. 下述（　　）密码算法与 SM2 算法使用相同的数学难题。
A、AES
B、RSA
C、ECDSA
D、DES
答案：C

48. SM2 算法的安全性基于（　　）困难假设。
A、双线性映射
B、椭圆曲线离散对数
C、多线性映射
D、丢番图方程求解
答案：B

49. 测评过程中，可以作为可能使用 SM2 加密的证据有（　　）。
A、密文比明文长 64 个字节
B、密文的第一部分是 SM2 椭圆曲线上的点
C、密文长度为 512 比特
D、加密公钥长度为 256 比特
答案：B

50. 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（　　）。
A、128 比特
B、256 比特
C、192 比特
D、512 比特
答案：B

51. 下列不属于 SM2 公钥加密算法特点的是（　）。
A、每次加密数据时，引入不同的随机数
B、可用于产生数字信封
C、解密过程可以验证结果正确性
D、密文比明文长 64 字节
答案：D

52. 公钥密钥密码体制往往基于一个（　）。
A、平衡布尔函数
B、杂凑函数
C、单向函数
D、陷门单向函数
答案：D

53. RSA 密码算法的安全性是基于（　　）。
A、离散对数问题的困难性
B、子集和问题的困难性
C、大整数因子分解的困难性
D、线性编码的解码问题的困难性
答案：C

54. 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（　　）。
A、Alice 的公钥
B、Alice 的私钥
C、Bob 的公钥
D、Bob 的私钥
答案：C

55. 公钥密码学的思想最早是由（　）提出的。
A、欧拉（Euler）
B、迪菲（Diffie）和赫尔曼（Hellman）
C、费马（Fermat）
D、里维斯特（Rivest）、沙米尔（Shamir）和埃德蒙（Adleman）
答案：B

56. PKI 主要基于的密码体制是（　　）。
A、对称密码
B、公钥密码
C、量子密码
D、密码杂凑算法
答案：B

57. 在现有的计算能力条件下，ElGamal 算法的最小密钥长度是（　　）。
A、128 位
B、160 位
C、512 位
D、1024 位
答案：D

58. 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。

A、Alice 的公钥
B、Alice 的私钥
C、Bob 的公钥
D、Bob 的私钥
答案：D

59. 利用公钥加密和私钥解密的密码体制是（　　）。
A、对称加密体制
B、非对称加密体制
C、轴对称加密体制
D、空间对称加密体制
答案：B

60. 下列的加密方案基于格理论的是（　　）。
A、ECC
B、RSA
C、AES
D、Regev
答案：D

61. SM2 算法中的（　　）算法已经进入 ISO 国际标准。
A、数字签名
B、公钥加密
C、密钥交换
D、身份认证
答案：A

62. SM2 算法中的密钥交换算法支持（　　）方密钥交换。
A、2
B、3
C、4
D、多
答案：A

63. 基域选择 256 比特素域时，SM2 算法的数字签名的长度为（　　）比特。
A、128
B、256
C、384
D、512
答案：D

64. 关于 RSA 公钥算法，下列说法错误的是（　　）。
A、RSA 加密算法中，公钥为（n，e）
B、RSA 加密算法中，公钥 e 与ϕ(n)互素
C、同等安全强度下，RSA 签名速度比 ECC 算法快
D、RSA 加密速度比解密速度快

答案：C

65. RSA-3072withSHA-224 的安全强度为（　　）比特。
A、80
B、112
C、128
D、192
答案：B

66. SM2 数字签名算法无法实现的功能是（　　）。
A、数据来源确认
B、消息机密性
C、签名者不可抵赖
D、数据完整性验证
答案：B

67. SM2 算法中计算量最大的运算是（　　）。
A、椭圆曲线点加
B、椭圆曲线倍点
C、椭圆曲线点乘
D、杂凑
答案：C

68. SM2 算法基于的椭圆曲线离散对数的计算复杂度为（　　）。
A、指数级
B、亚指数级
C、超指数级
D、超多项式
答案：A

69. SM2 算法采用的素域椭圆曲线构成的数学结构是（　　）。
A、交换群
B、非交换群
C、环
D、域
答案：A

70. SM2 算法采用的素域椭圆曲线的基本参数不包括（　　）。
A、域的规模
B、基点的阶
C、基点
D、无穷远点
答案：D

71. SM2 算法基于椭圆曲线上的点乘计算的计算复杂度为（　　）。
A、线性级

B、多项式级
C、超多项式级
D、亚指数级
答案：D

72. SM2 算法采用的椭圆曲线上的无穷远点是群的（　　）点。
A、0
B、最大点
C、基点
D、1
答案：A

73. SM2 算法公开参数中的基点是（　　）。
A、椭圆曲线群的 0 点
B、椭圆曲线群的生成元
C、椭圆曲线群的最大点
D、基域的生成元
答案：B

74. SM2 算法中的公钥加密算法的公钥是（　　）。
A、基域的元素
B、椭圆曲线上的随机点
C、椭圆曲线的 0 点
D、椭圆曲线的基点
答案：B

75. 加密密钥和解密密钥为同一密钥的密码算法。这样的加密算法称为（　　）。
A、非对称密码
B、单密钥密码
C、对称密码
D、序列密码
答案：B

76. SM9 是一种（　　）算法。
A、序列密码
B、分组密码
C、公钥密码
D、杂凑函数
答案：C

77. （　　）是 SM9 密码算法的特点。
A、基于数字证书
B、抗量子计算攻击
C、基于标识
D、安全性基于大数分解问题难解性
答案：C

78. 以下（　　）不能作为 SM9 密码算法的标识。
A、姓名
B、身份证号
C、手机号码
D、电子邮箱
答案：A

79. SM9 密钥交换协议的辅助函数不包括（　　）。
A、杂凑函数
B、密钥派生函数
C、随机数发生器
D、分组密码算法
答案：D

80. （　　）算法是基于标识的密码算法。
A、SM2
B、SM3
C、SM4
D、SM9
答案：D

81. SM9 密码算法系统参数不包括（　　）。
A、椭圆曲线方程参数
B、私钥生成函数识别符
C、椭圆曲线识别符
D、双线性对识别符
答案：B

82. SM9 密码算法椭圆曲线无穷远点的字节串表示形式是（　　）。
A、单一零字节表示形式
B、压缩表示形式
C、未压缩表示形式
D、混合表示形式
答案：A

83. 关于 SM9 密码算法选用椭圆曲线的嵌入次数说法正确的是（　　）。
A、嵌入次数越大安全性越高
B、嵌入次数越大双线性对计算越容易
C、选择椭圆曲线的嵌入次数越大越好
D、选择椭圆曲线的嵌入次数越小越好
答案：A

84. SM9 密码算法采用的椭圆曲线双线性对是（　　）。
A、Weil 对
B、Tate 对

C、Ate 对
D、R-ate 对
答案：D

85. SM9 密码算法采用的椭圆曲线的嵌入次数是（　　）。
A、10
B、11
C、12
D、13
答案：C

86. （　　）算法可用于做 SM9 数字签名算法的辅助函数。
A、SM1
B、SM2
C、SM3
D、SM4
答案：C

87. SM9 数字签名的生成会用到（　　）。
A、主公钥
B、主私钥
C、标识
D、数字证书
答案：A

88. SM9 密码算法用户公钥（　　）。
A、通过随机数发生器生成
B、根据用户标识唯一确定
C、通过主私钥结合系统参数生成
D、通过用户私钥结合系统参数生成
答案：B

89. SM9 密码算法的功能不包括（　　）。
A、数字签名
B、密钥交换
C、杂凑函数
D、公钥加密
答案：C

90. 在 SM9 数字签名的生成和验证过程之前，杂凑函数（　　）。
A、仅对待签名消息进行压缩
B、仅对待验证消息进行压缩
C、对待签名消息和待验证消息都要压缩
D、不起任何作用
答案：C

91. SM9 密钥封装机制封装的秘密密钥是（　　）生成的。
A、根据主公钥
B、根据接受者的用户标识
C、由随机数发生器
D、以上都不对
答案：B

92. 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。
A、S 盒
B、伪随机数生成器
C、密钥流
D、线性函数
答案：B

93. 下面不是公钥密码算法可依据的难解问题的是（　　）。
A、大整数分解问题（简称 IFP）
B、离散对数问题（简称 DLP）
C、椭圆曲线离散对数问题（简称 ECDLP）
D、置换-代换
答案：D

94. 数字信封是用来解决（　　）。
A、公钥分发问题
B、私钥分发问题
C、对称密钥分发问题
D、数据完整性问题
答案：C

95. 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。
A、主模式
B、快速模式
C、传输模式
D、隧道模式
答案：D

96. 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 IPSecSA 实现双向通信，这样设计可以防范（　　）。
A、重放攻击
B、中间相遇攻击
C、中间人攻击
D、侧信道攻击
答案：A

97. 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（　　）。

A、RSA 算法用于实现身份鉴别
B、基于 RSA 数字信封方式进行密钥交换
C、AES-GCM 算法用于实现通信数据机密性保护
D、AES-GCM 算法用于实现通信数据完整性保护
答案：B

98. 以下最适合用于支持 NAT（网络地址转换）穿越的模式是（　　）。
A、传输模式下使用 AH+ESP 协议
B、隧道模式下使用 AH+ESP 协议
C、传输模式下使用 ESP 协议
D、隧道模式下使用 ESP 协议
答案：D

99. 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。
A、传输层
B、链路层
C、网络层
D、应用层
答案：D

100. 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。
A、安全性
B、完整性
C、可靠性
D、机密性
答案：B

101. 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（　　）。
A、输入序列是统计独立的
B、输出速率是稳定的
C、输入序列会被压缩输出
D、输入序列是不均衡的
答案：B

102. 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（　　）。
A、密钥建立协议
B、密钥传输协议
C、密钥共享协议
D、密钥协商协议
答案：D

103. 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（　　）。
A、DH 协议

B、MQV 协议
C、ECDH 协议
D、数字信封技术
答案：A

104. 如果有 6 个成员组成的团体希望互相通信，那么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（　　）。
A、5
B、8
C、6
D、15
答案：C

105. 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（　　）。
A、密钥托管技术
B、门限密钥协商技术
C、密钥分发技术
D、门限秘密共享技术
答案：D

106. 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。
A、交换
B、存储
C、延续
D、删除
答案：B

107. 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（　　）。
A、代理签名
B、群签名
C、多重签名
D、盲签名
答案：D

108. 一个数字签名体制包含的内容，说法正确的是（　　）。
A、包含加密和解密两个方面
B、包含加密和认证两个方面
C、包含签名和验证签名两个方面
D、包含认证和身份识别两个方面
答案：C
109. 关于数字签名，以下说法正确的是（　　）。
A、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

B、数字签名能够解决数据的加密传输，即安全传输问题
C、数字签名一般采用对称加密机制
D、数字签名能够解决篡改、伪造等安全性问题
答案：D

110. 下面对于数字签名的描述不正确的是（　　）。
A、数字签名是可信的
B、数字签名是不可抵赖的
C、数字签名是可伪造的
D、数字签名是不可伪造的
答案：C

111. 下面的说法中错误的是（　　）。
A、对称密码系统的加密密钥和解密密钥相同
B、PKI 系统的加密密钥和解密密钥不同
C、数字签名之前要先对消息或报文做摘要
D、数字签名系统一定具有数据加密功能
答案：D

112. 下面有关盲签名说法错误的是（　　）。
A、消息的内容对签名者是不可见的
B、在签名被公开后，签名消息一定可追踪
C、消息的盲化处理由消息拥有者完成
D、满足不可否认性
答案：B

113. 下面有关群签名说法错误的是（　　）。
A、只有群成员能代表这个群组对消息签名
B、验证者可以确认数字签名来自于该群组
C、验证者能够确认数字签名是哪个成员所签
D、借助于可信机构可以识别出签名是哪个签名人所为
答案：C

114. 与 RSA 算法相比，DSS（数字签名标准）不包括（　　）。
A、数字签名
B、鉴别机制
C、加密机制
D、数据完整性
答案：C

115. 签名者把他的签名授权给某个人，这个人代表原始签名者进行签名，这种签名称为（　　）。
A、代理签名
B、群签名
C、多重签名
D、盲签名

答案：A

116. 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。
A、加密
B、数字签名
C、数字认证
D、秘密共享
答案：B

117. 关于 SM9 数字签名算法以下说法错误的是（　）。
A、基于椭圆曲线双线性对实现
B、签名之前需要对待签消息进行压缩
C、使用主私钥对待签消息进行签名
D、可通过签名者标识和其他信息对签名进行验证
答案：C

118. 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（　）。
A、代理签名
B、群签名
C、多重签名
D、盲签名
答案：D

119. 下列方法通常用来实现抗抵赖性的是（　）。
A、加密
B、数字签名
C、时间戳
D、哈希值
答案：B

120. 下列不属于数字签名所能实现的安全保证的是（　）。
A、保密通信
B、防抵赖
C、防冒充
D、防伪造
答案：A

121. PKI 体系所使用数字证书的格式标准是（　）。
A、RSA
B、PGP
C、X.509
D、ECC
答案：C

122. PKI 是（　　）的简称。
A、Private KeyInfrastructure
B、Public KeyInfrastructure
C、Public Key Institute
D、Private Key Institute
答案：B

123. 下面哪个格式描述了证书请求语法（　　）。
A、PKCS#7
B、PKCS#8
C、PKCS#9
D、PKCS#10
答案：D

124. 以下哪项不是 CA 的服务功能（　　）。
A、提供加密私钥管理
B、用户证书签发
C、用户证书撤销
D、用户证书查询
答案：A

125. 公钥密码体制中，其他人可以用公钥进行（　　）。
A、加密和验证签名
B、解密
C、签名
D、以上均不对
答案：A

126. 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（　　）。
A、主体的解密密钥
B、证书序列号摘要
C、密钥交换协议
D、签名值
答案：D

127. 数字证书由 CA 机构签发，用（　　）来验证证书。
A、私钥
B、公钥
C、SRA
D、序列号
答案：B

128. 在 PKI 系统中，由（　　）绑定用户的身份信息和公钥。
A、发送方
B、CA 机构

C、接收方
D、不需要
答案：B

129. CA 用（ ）签名数字证书。
A、用户的公钥
B、用户的私钥
C、自己的公钥
D、自己的私钥
答案：D

130. 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（ ）。
A、数字签名
B、加密技术
C、生物识别
D、实体鉴别
答案：A

131. 下面有关数字签名描述错误的是（ ）。
A、通过待签名消息、签名值和公钥完成签名验证
B、发送者事后不能抵赖对报文的签名
C、接收者不能伪造签名
D、能够保证待签名消息的机密性
答案：D

132. 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。
A、检查根证书如何安全导入或预置到系统内
B、检查数字证书的合规性
C、验证数字证书的证书链是否通过
D、检查数字证书的机密性是如何保证的
答案：D

133. 以下选项（ ）不是对传输完整性实现的测评方法。
A、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
B、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
C、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
D、检查传输过程是否符合 GB/T15843《信息技术 安全技术实体鉴别》要求
答案：D

134. 确保信息仅被合法实体访问，而不被泄露给非授权的实体或供其利用的特性是指信息的（ ）。

A、保密性
B、完整性
C、可用性
D、不可否认性
答案：A

135. 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。
A、MD5
B、Blowfish
C、SHA-256
D、SHA-512
答案：A

136. 在测评过程中遇到的 PEM 编码格式，除了开头和结尾，其内容通常以（　　）格式编码。
A、BER
B、DER
C、Base64
D、Base64url
答案：C

137. 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（　　）。
A、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”
B、若 CSP 机房通过密评，则可以复用该机房的密评结论
C、若 CSP 机房未通过密评，则可以直接判定为“符合”
D、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”
答案：B

138. 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（　　）。
A、符合
B、部分符合
C、不符合
D、不适用
答案：C

139. 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（　　）。

A、符合
B、部分符合
C、不符合
D、不适用
答案：C

140. 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（　　）。
A、符合，1 分
B、部分符合，0.5 分
C、部分符合，0.3 分
D、不符合，0.25 分
答案：B

141. 以下因素（　　）可能导致数字签名功能不正确。
A、签名中使用固定的随机数
B、待签消息比 SM3 杂凑值长
C、签名中使用不可预测的随机数
D、使用私钥签名
答案：A

142. 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（　　）。
A、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
B、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
C、开发人员不可能使用 ECB 模式加密
D、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
答案：A

143. 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（　　）。
A、采用 ECDHE 算法进行密钥协商
B、采用 RSA 算法来保证通信过程中数据的机密性
C、采用 AES 算法来保证通信过程中数据的完整性
D、采用 SHA 算法来保证通信过程中数据的完整性
答案：A

144. 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。

A、核心密码
B、普通密码
C、商用密码
D、核心密码和普通密码
答案：C

145. 下面算法运算时不需要密钥的是（ ）。
A、SM2
B、SM4
C、ZUC
D、SM3
答案：D

146. 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（ ）。
A、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
B、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
C、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
D、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
答案：A

147. SM2 算法中的数字签名的签名运算最耗时的是（）运算。
A、随机数生成
B、消息映射
C、素性检测
D、点乘
答案：D

148. 基域选择 Fp-256 时，SM2 算法的数字签名的私钥长度为（ ）。
A、128
B、256
C、384
D、512
答案：B

149. （ ）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。
A、SM2 签名
B、DSA
C、RSA-PSS 签名
D、EdDSA
答案：D

150. 在区块链中，用户的交易记录会通过区块的方式进行组织，然后通过一种块链结构将区块串联在一块，形成区块链账本。以下（ ）可用于区块链账本的存储安全管理。
A、通过 SHA1 算法计算区块头的杂凑值标识区块，用于链接相邻区块
B、采用 SM4 算法保证账本重要内容的机密性
C、只通过用户名、口令实现访问账本数据的身份鉴别
D、采用 MD5 算法保证账本重要内容的完整性
答案：B

151. 某物联网智慧水务系统需实现低功耗终端设备与云端的安全通信，要求满足以下条件：
（1）终端计算能力弱，需轻量级算法加密水质传感数据流（每秒 1KB）；
（2）通信双方需完成双向身份认证，防止伪造节点接入；
（3）数据完整性需抗重放攻击，且传输时延低于 50ms。
以下哪种算法组合最符合需求？（ ）
A、 SM2 + SM3 + CBC 模式填充
B、 SM4-CTR + SM3-HMAC +预共享 SM9 密钥
C、 ZUC 流加密+ SM2 数字签名+ SM3 哈希
D、SM4-OFB + SM3-KDF +动态 SM2 证书
答案：B

152. 某科技公司想要使用密码技术对其开发的线上会议系统的实时视频流进行加密传输，使用以下哪种密码算法可以最大限度保证视频流的实时性（ ）
A、ZUC
B、SM2
C、SM3
D、RSA
答案：A

153. Alice 有一台专用加密机，其只能实现 ZUC 算法。Alice 使用该加密机，一定无法实现的功能是（ ）
A、真实性
B、机密性
C、完整性
D、不可否认性
答案：D

154. 在 5G 通信的加密场景中，ZUC 算法被用于生成密钥流。以下关于 ZUC 算法核心结构的描述正确的是（ ）
A、采用 256 位初始密钥
B、包含 16 级线性反馈移位寄存器(LFSR)
C、每轮输出 64 位密钥流
D、其 S 盒设计基于 AES 的 SubBytes 变换
答案：B
155. Alice 对某数据传输的加密代码进行分析，发现其是通过提前生成密钥流再与明文逐比特异或的方式对数据进行加密的。那么，其所使用的密码算法可能是

（ ）
A 、AES
B 、SM4
C 、ZUC
D 、MD5
答案：C
156. 某公司计划研发一套嵌入式设备，需要对该设备传输的数据通过密码技术进行加密，并在传输对端进行解密，该设备的计算资源有限，且实时性要求较高，使用如下哪种密码算法可更好适配该场景（ ）
A 、MD5
B 、SM2
C 、SM3
D 、ZUC
答案：D
157. 当安全技术人员检查 5G 核心网时，发现加密模块的初始化向量(IV)固定不变。这会导致（ ）
A、加密速度下降
B、相同密钥下密钥流重复
C、数据明文传输
D、触发基站重启保护
答案：B
158. 某智能电表项目要求使用国密算法进行通信加密，工程师选择 ZUC 算法而不使用其他的国密算法是因为（ ）
A、适合低功耗嵌入式设备
B、支持 512 位超长密钥
C、内置纠错编码功能
D、可替进行数字签名
答案：A

159. 工程师调试 ZUC 硬件模块时，发现首次输出的 32 位密钥流全为 0，应优先检查（ ）
A、电源供电电压
B 、LFSR 初始化状态
C、散热片安装情况
D、晶振频率偏差
答案：B

160. 某无人机在传输视频信号时使用了 ZUC-256，而非 ZUC 的标准版，ZUC-256 相比标准版本主要增强了（ ）
A、抗侧信道攻击能力
B、密钥派生函数强度
C、算法吞吐量
D、密钥空间大小
答案：D

161. Alice 破解了某系统的对存储数据进行加密的源代码，发现其是使用 ECB

模式对数据进行加密存储的。那么可以分析得出，该系统最不可能是使用下列的哪类密码算法实现数据存储的机密性保护的（　）
A、 ZUC
B 、SM4
C、 AES
D 、DES
答案：A

162. 某金融机构计划升级跨境支付系统，需在区块链底层实现以下安全功能：
（1）节点间密钥协商支持后量子安全特性；
（2）交易哈希算法需抗长度扩展攻击；
（3）智能合约权限管理需支持属性基细粒度控制；
（4）兼容现有国际标准的同时优先采用国密算法。
应选择哪种技术方案？（　）
A、ECDH+ SHA-256 +基于 SM2 的访问控制
B、SM2-KEM+ SM3 +SM9 属性基加密
C、Kyber + SM3 + SM4 工作流加密
D、SM9 密钥交换+ BLAKE2s + SM2 属性签名
答案：B

二、多选题 158
1. 雪崩效应指加密算法的一种理想属性，当输入发生最微小的改变时，也会导致输出的剧变。下列密码算法中具有雪崩效应的是（　）。
A、RSA
B、AES
C、DES
D、MD5
答案：BCD

2. 线性反馈移位寄存器（LFSR）是常见的密码算法部件，以下密码算法中未使用到 LFSR 的是？（　）
A、ZUC
B、SM2
C、SM3
D、SM4
答案：BCD

3. 某公司着手在偏远山区建设 5G 基站，计划在加密模块中使用 ZUC 算法，可能是由于 ZUC 包含下列哪些特点（　）。
A、硬件实现面积小，适合嵌入式设备
B、抗量子计算攻击能力突出
C、符合 3GPP 标准
D、可实现数字签名保证不可否认性
答案：AC

4. 某开发单位依据 GM/T 0001-2012 使用 ZUC 算法对其系统数据进行机密性保

护，下列做法错误的有（　）
A、使用 64 位密钥
B、自定义 S 盒
C、在 LFSR 中使用 16 个 32 比特寄存器
D、初始化阶段进行 16 轮迭代
答案：ABCD

5. Alice 发现，自己运维的信息系统 ZUC 密钥流异常重复，为解决该问题，采取的措施包含（　）
A、立即更换初始密钥
B、检查 IV 生成模块随机性
C、改用 CBC 模式的 ZUC
D、立即更换 ZUC 算法的数字证书
答案：AB

6. 某团队实现 ZUC 时的错误做法包括（　）
A、为节省内存复用 IV 和密钥
B、IV 固定为全 0
C、不使用比特重组部分
D、为提升效率每拍输出 128 比特的密钥字
答案：ABCD

7. 在分组密码设计中用到扩散和混淆的理论。理想的扩散是（　）。
A、明文的一位只影响密文对应的一位
B、让密文中的每一位受明文中每一位的影响
C、让明文中的每一位影响密文中的所有位。
D、一位明文影响对应位置的密文和后续密文
答案：BC

8. 1976 年，提出公钥密码学系统的学者是（　）。
A、Diffie
B、Shami
C、Hellman
D、Hill
答案：AC

9. 下列选项属于针对密码协议的常见攻击方法的是（　）。
A、重放攻击
B、并行会话攻击
C、中间人攻击
D、预言者会话攻击
答案：ABCD

10. 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（　）。
A、最短向量问题 (Shortest Vector Problem， SVP)

B、最近向量问题，Closest Vector Problem）
C、容错学习（Learning With Errors， LWE)
D、最小整数解（Small Interger Solution)
答案：ABCD

11. 密码学发展的三个阶段（ ）。
A、代换、置换密码
B、古典密码
C、近代密码
D、现代密码
答案：BCD

12. 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（ ）。
A、RSA
B、DSA
C、AES
D、SM3
答案：AB

13. 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（ ）。
A、加密算法
B、解密算法
C、密文
D、密钥
答案：ABC

14. 与量子密码相对应，经典密码学包括（ ）。
A、密码编码学
B、密码分析学
C、后（抗）量子密码学
D、量子密码
答案：AB

15. 下列哪些参数决定了穷举攻击所消耗的时间（ ）。
A、密钥空间
B、密钥长度
C、主机运算速度
D、主机显存容量
答案：ABC

450 重复
16. 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（ ）。
A、智能卡
B、USB Key

C、密码加速卡
D、安全芯片
答案：ABCD

17. 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（ ）。
A、RC4 和 RC5
B、RSA 和 DSA
C、SM4 和 AES
D、SM2 和 SM9
答案：ABCD

18. 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（ ）。
A、输入 x 可以为任意长度；输出数据串长度固定
B、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）
C、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
D、可以找到两个消息 x、y，使得 H（x）=H（y）
答案：ABC

19. 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（ ）。
A、基于密钥安全
B、加解密算法公开
C、加密算法保密
D、基于置换算法
答案：AB

20. 根据有限域的描述，下列（ ）是有限域。
A、模素数 n 的剩余类集
B、GF（2 的 8 次方）
C、整数集
D、有理数集
答案：AB

21. 以下关于完整性保护的说法错误的有（ ）。
A、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
B、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
C、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
D、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
答案：BC

22. 以下场景利用了密码的不可否认功能的是（　）。
A、网银用户对交易信息进行签名
B、电子证照
C、服务端对挑战值进行签名
D、SSL 协议中对会话计算 MAC
答案：AB

23. 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（　）。
A、RSA 算法
B、ElGamal 算法
C、AES 算法
D、ECC（椭圆曲线密码）算法
答案：ABD

24. SM4 算法的轮函数包括的运算有（　）。
A、异或
B、非线性变换
C、线性变换
D、相乘
答案：ABC

25. AES 分组密码算法密钥长度可以是（　）。
A、56 比特
B、128 比特
C、192 比特
D、256 比特
答案：BCD

26. 下列（　）不属于分组密码体制。
A、ECC
B、IDEA
C、RC5
D、ElGamal
答案：AD

27. 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（　）。
A、XTS
B、HCTR
C、CTR
D、ECB
答案：ABC

28. 以下（　）算法可以安全地为变长的数据生成 MAC。
A、CBC-MAC

B、HMAC
C、GCM
D、CMAC
答案：BCD

29. 下列关于分组密码算法的设计的说法正确的是（ ）。
A、分组长度应足够大，以防止明文被穷举攻击
B、密钥空间应足够 大，尽可能消除弱密钥
C、密钥越长，安全性越强，因此，设计的密钥长度应该很长
D、由密钥确定的算法要足够复杂，要能抵抗各种已知的攻击
答案：ABD

30. 在 SM4 算法的线性变换中，循环左移运算的移位数包括（ ）。
A、2
B、10
C、18
D、24
答案：ABCD

31. 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。
A、扩展置换
B、初始置换
C、非线性变换
D、线性变换
答案：CD

32. 下述（ ）算法的 S 盒与 SM4 算法的 S 盒是仿射等价。
A、DES
B、AES
C、Camellia
D、MISTY
答案：BC

33. 下述正确描述 SM4 的是（ ）。
A、SM4 目前 ISO/IEC 标准化组织采纳
B、SM4 的分组长度为 128 位
C、SM4 的密钥长度为 128 位
D、SM4 原名 SMS4
答案：ABCD

34. 下列分组密码工作模式中，解密过程支持并行计算的有（ ）。
A、CBC
B、CTR
C、ECB
D、XTR
答案：ABC

35. 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。
A、保护数据机密性
B、保护数据完整性
C、不可否认性
D、运行速度快
答案：ACD

36. 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（ ）。
A、CBC
B、OFB
C、CFB
D、CTR
答案：BCD

37. 下列分组密码可鉴别的加密模式，使用串行结构的包括（ ）。
A、OMAC
B、XCBC
C、PMAC
D、EMAC
答案：ABD

38. 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（ ）。
A、Nonce
B、密文
C、标签
D、密钥
答案：BC

39. 分组密码的短块加密方法主要有（ ）。
A、填充法
B、序列密码加密法
C、输出反馈模式
D、密文挪用技术
答案：ABD

40. 以下关于分组密码正确说法的是（ ）。
A、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
B、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
C、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
D、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
答案：ACD

41. 以下分组密码的工作模式类似于流密码的是（　）。
A、CFB
B、CBC
C、CTR
D、OFB
答案：ACD

42. ZUC 算法中使用到的运算包括（　）。
A、模 2^{31}-1 的加法
B、模 2^{32}的加法
C、右循环移位
D、左循环移位
答案：ABD

43. 关于 ZUC 算法初始化过程描述正确的是（　）。
A、迭代 64 轮
B、初始化完成后直接输出密钥流
C、迭代 32 轮
D、非线性函数的输出会参与 LFSR 的反馈运算
答案：CD

44. 基于 ZUC 算法的完整性算法工作流程中的步骤有（　）。
A、初始化
B、函数扩展
C、产生密钥流
D、计算 MAC
答案：ACD

45. 下列属于序列密码算法的是（　）。
A、RC4
B、A5
C、SEAL
D、SNOW2.0
答案：ABCD

46. 以下关于 SM3 密码杂凑算法和 SHA-256 的描述正确的是（　）。
A、消息字的介入方式相同
B、消息扩展过程生成的总消息字个数相同
C、杂凑值的长度相同
D、压缩函数的轮数
答案：CD

47. SM3 密码杂凑算法的运算中（　）起到混淆的作用。
A、循环移位
B、P 置换
C、模加

D、布尔函数
答案：CD

48. 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（　）。
A、MD5
B、SHA-1
C、SHA-256
D、SM3
答案：CD

49. 下列属于对密码杂凑函数的攻击方法是（　）。
A、生日攻击
B、暴力破解攻击
C、已知明文攻击
D、选择密文攻击
答案：AB

50. 密码杂凑算法的安全特性包括（　）。
A、单向性
B、抗弱碰撞
C、抗强碰撞
D、抗伪造
答案：ABC

51. 下面关于 SHA-1 的附加填充位操作，说法正确的是（　）。
A、填充一个 1 和若干个 0
B、在消息后附加 32bit 的无符号整数
C、长度模 512 与 448 同余
D、填充后的消息长度为 512 比特的整数倍
答案：ACD

52. 单向杂凑函数可以用于以下哪些方面（　）。
A、数字签名
B、密钥共享
C、消息完整性检测
D、操作系统中账号口令的安全存储
答案：ABCD

53. 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（　）。
A、弱碰撞自由的杂凑函数
B、强碰撞自由的杂凑函数
C、强杂凑函数
D、弱杂凑函数
答案：AB

54. 攻击杂凑函数的方法有（　）。

A、穷举攻击法
B、生日攻击
C、中途相遇攻击
D、近源攻击
答案：ABC

55. 公钥密码算法使用两个密钥，下述描述正确的是（　）。
A、一个是公钥，一个是私钥
B、一个是加密密钥，一个是解密密钥
C、一个是公开的密钥，一个是秘密保存的私钥
D、一个用于加密，一个用于 MAC
答案：ABC

56. SM2 的安全特性主要体现在（　）方面。
A、算法具备单向性
B、密文不可区分性
C、密文具有抗碰撞性
D、密文具有不可延展性
答案：ABCD

57. 相对于对称加密算法，非对称密钥加密算法通常（　)。
A、加密速率较低
B、更适合于数据的加解密处理
C、安全性一定更高
D、加密和解密的密钥不同
答案：AD

58. 列属于后量子公钥密码研究方向的是（　）。
A、多变量公钥密码
B、基于格的公钥密码
C、基于纠错码的公钥密码
D、基于椭圆曲线离散对数困难问题的公钥密码
答案：ABC

59. 关于 RSA 的参数选择，正确的是（　）。
A、选取两个秘密素数 p 和 q
B、选取两个公开素数 p 和 q
C、（p-1）和（q-1）都必须至少具有一个很大的素因数
D、p 和 q 二者之差不宜过小
答案：ACD

60. M2 公钥加密算法可以抵抗的攻击包括（　）。
A、唯密文攻击
B、选择明文攻击
C、选择密文攻击
D、密钥恢复攻击

答案：ABCD

61. 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（　）。
A、RSA
B、SM2
C、ECDSA
D、NTRU
答案：BC

62. SM2 公钥密码算法一般包括如下哪些功能（　）。
A、密钥派生
B、签名
C、密钥交换
D、加密
答案：BCD

63. 有关 SM9 标识密码算法描述错误的是（　）。
A、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
B、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
C、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
D、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
答案：AC

64. SM9 密码算法 KGC 是负责（　）的可信机构。
A、选择系统参数
B、生成主密钥
C、生成用户标识
D、生成用户私钥
答案：ABD

65. SM9 密码算法椭圆曲线非无穷远点的字节串表示形式有（　）。
A、单一零字节表示形式
B、压缩表示形式
C、未压缩表示形式
D、混合表示形式
答案：BCD

66. 密钥派生函数是（　）算法的辅助函数。
A、SM9 数字签名
B、SM9 密钥交换
C、SM9 密钥封装

D、SM9 公钥加密
答案：BCD

67. （ ）算法需要密钥派生函数作为辅助函数。
A、SM9 数字签名
B、SM9 密钥交换
C、SM9 密钥封装
D、SM9 公钥加密
答案：BCD

68. 公钥密码体制的基本思想包括（ ）。
A、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
B、加密密钥公开，解密密钥保密
C、由加密密钥推出解密密钥，在计算上是不可行的
D、以上都不对
答案：BC

69. SM2 算法涉及到的运算有（ ）。
A、椭圆曲线点乘
B、散列值计算
C、椭圆曲线点加
D、随机数生成
答案：ABCD

70. RSA 密码体制中用到了（ ）等数论知识。
A、Euclidean 算法
B、中国剩余定理
C、费马小定理
D、欧拉函数
答案：ABCD

71. 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（ ）。
A、机密性
B、可用性
C、真实性
D、完整性
答案：ACD

72. 根据密钥信息的交换方式，密钥分发可以分为（ ）两类。
A、人工（离线）密钥分发
B、自动（在线）密钥分发
C、固定密钥分发
D、随机密钥分发
答案：AB

73. 以下哪些密码系统的参数应该与密钥一样进行保护（　）。
A、SM4 加密过程中的轮密钥
B、密码算法中随机数发生器的内部状态
C、椭圆曲线密码体制所使用的域的参数
D、SM2 密钥交换临时产生的随机数
答案：ABD

74. 以下关于密钥派生的说法正确的有（　）。
A、从口令派生密钥可用于加密存储设备
B、从口令派生密钥可用于网络通信数据保护
C、可以基于 HMAC 算法实现
D、可以基于 CMAC 算法实现
答案：AC

75. 关于消息认证，以下说法正确的是（　）。
A、可以验证消息来源
B、可以验证消息的完整性
C、可以验证消息的真实性
D、可以加密消息
答案：ABC

76. 盲签名与普通签名相比，其显著特点为（　）。
A、签名者是用自己的公钥进行签名
B、签名者不知道所签署的数据内容
C、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
D、在签名被接收者泄露后，签名者不能跟踪签名
答案：BD

77. 证书的生命周期包括以下哪些（　）。
A、证书申请
B、证书生成
C、证书存储
D、证书撤销
答案：ABCD

78. PKI 的基本组成包括（　）。
A、CA
B、KM
C、RA
D、密钥分发中心
答案：ABC

79. 对用户的身份鉴别基本方法可以分为（　）。
A、基于虹膜的身份鉴别
B、基于秘密信息的身份鉴别
C、基于指纹的身份鉴别

D、基于人脸的身份鉴别
答案：ABCD

80. 我国涉密人员分为（ ）。
A、核心涉密人员
B、非常重要涉密人员
C、重要涉密人员
D、一般涉密人员
答案：ACD

81. 常见的后量子密码（或抗量子密码）技术的研究领域主要包括（ ）。
A、基于编码后量子密码
B、基于多变量后量子密码
C、基于格后量子密码
D、基于杂凑算法后量子密码
答案：ABCD

82. 我国 SM2 公钥密码算法包含的 3 个算法是（ ）。
A、数字签名算法
B、密钥封装算法
C、密钥交换协议
D、公钥加密解密算法
答案：ACD

83. 评价密码系统安全性主要有以下哪些方法？（ ）
A、计算安全性
B、无条件安全性
C、加密安全性
D、可证明安全性
答案：ABD

84. 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（ ）。
A、证实消息的信源
B、证实消息内容是否被篡改
C、保护消息的机密性
D、保护用户隐私
答案：AB

85. 古典密码体制的分析方法有（ ）。
A、统计分析法
B、明文-密文分析法
C、穷举分析法
D、重合指数法
答案：ABCD

86. 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。
A、2DES
B、3DES
C、4DES
D、5DES
答案：AB

87. AES 分组密码算法加密过程的轮数可以是（ ）。
A、10 轮
B、12 轮
C、14 轮
D、16 轮
答案：ABC

88. 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。
A、保护数据机密性
B、保护数据完整性
C、数据起源认证
D、运行速度快
答案：BC

89. 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（ ）。
A、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
B、如果明文和密钥一定时，则每次 ECC 加密的密文一定相同
C、如果明文和密钥一定时，则每次 ElGamal 加密的密文一定相同
D、以上都不对
答案：A

90. 以下哪种算法属于分组密算法的是（ ）。
A、IDEA
B、RC4
C、Blowfish
D、RC5
答案：ACD

91. 以 ZUC 算法为核心，成为 3GPP LTE 标准的算法为（ ）。
A、128EEA-3
B、128EIA-3
C、128UEA-3
D、128UIA-3
答案：AB

92. 关于 ZUC 算法描述正确的是（ ）。

A、3GPP LTE 唯一标准
B、基于素域上的 LFSR 设计
C、算法结构新颖
D、算法软硬件实现性能良好
答案：BCD

93. 下列选项中可能涉及密码杂凑运算的是（)。
A、消息机密性
B、消息完整性
C、消息鉴别码
D、数字签名
答案：BCD

94. 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（ ）。
A、MD4
B、RIPEMD
C、SM3
D、SHA-0
答案：ABD

95. 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（ ）。
A、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
B、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
C、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
D、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
答案：ABD

96. 在公钥密码体制中，用于加密运算的密钥为（）。
A、公钥
B、私钥
C、公钥或私钥
D、以上都不对
答案：A

450 重复
97. 下列关于 SHA-3 的说法正确的是（ ）。
A、SHA-3 是基于 Sponge 结构设计的
B、不限定输入消息的长度
C、输出消息的长度根据需要可变

D、适用于 SHA-1 的攻击方法也可以作用于 SHA-3
答案：AB

98. SM2 算法与（ ）算法属于同一类数学结构。
A、ECDH
B、RSA
C、ECDSA
D、SM9
答案：ACD

99. 以下不是背包公钥加密体制的是（ ）。
A、LWE
B、ECC
C、Merkle-Hellman
D、McEliece
答案：ABD

100. 相对于对称密码算法，公钥密码算法的特点是（ ）。
A、加密速度慢
B、更适合于批量数据加解密处理
C、加密速度快
D、加密和解密的密钥不同
答案：AD

101. 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（ ）。
A、签名值中，r 的最高位为 1，s 的最高位为 0
B、签名值中，r 的最高位为 0，s 的最高位为 1
C、签名值中，r 的最高位为 0，s 的最高位为 0
D、签名值中，r 的最高位为 1，s 的最高位为 1
答案：AB

102. SM9 密码算法的特点有（ ）。
A、抗量子计算攻击
B、基于椭圆曲线双线性对
C、基于标识
D、基于数字证书
答案：BC

103. SSL 协议可以实现的安全需求有（ ）。
A、服务器对用户身份认证
B、用户对服务器身份认证
C、传输信息的机密性
D、传输信息的完整性
答案：ABCD

104. 以下关于 SSL/TLS 说法，正确的是（ ）。
A、使用 SSL/TLS 可以确保通信报文的机密性
B、在 SSL/TLS 中，使用数字签名技术来认证通信双方的身份
C、在 SSL/TLS 中，可以确保通信报文的完整性
D、在 SSL/TLS 中，一定是实现了双向身份鉴别
答案：ABC

105. 在密钥分发场景中，常见做法有（ ）。
A、人工传递
B、知识拆分
C、通过密钥加密密钥（KEK）加密传输
D、数字信封
答案：ABCD

106. 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（ ）。
A、客户端对 SSL VPN 服务端的身份鉴别
B、SSL VPN 服务端对客户端使用智能密码钥匙的身份鉴别
C、第三方电子认证服务
D、身份鉴别过程是否采用了挑战响应机制
答案：ABD

107. 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（ ）。
A、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
B、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
C、两个安全层面的数据保护对象不一样
D、两个安全层面可以相互弥补，降低风险
答案：ABCD

108. 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（ ）
A、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。
B、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。
C、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。
D、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
答案：ACD

109. 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（ ）。
A、堡垒机与设备之间的通信信道
B、浏览器与堡垒机之间的通信信道
C、浏览器与设备之间的通信信道
D、设备与设备之间的通信信道
答案：AB

110. 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（ ）。
A、用户注册业务
B、商品交易业务
C、交易订单数据
D、用户浏览记录
答案：ABCD

111. 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（ ）。
A、用户注册信息
B、智能密码钥匙
C、服务器密码机
D、数据库服务器
答案：AC

112. 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（ ）。
A、判定通用服务器和数据库为部分符合
B、判定通用服务器和数据库为不符合
C、判定通用服务器和数据库采取了风险缓解措施
D、判定通用服务器和数据库为高风险
答案：BC

113. 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（ ）。
A、互联网国密浏览器与前台应用系统之间的通信信道
B、互联网国密浏览器与后台管理系统之间的通信信道
C、互联网非国密浏览器与前台应用系统之间的通信信道
D、互联网非国密浏览器与后台管理系统之间的通信信道
答案：AC

114. 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（ ）。
A、SSL VPN 安全网关
B、USBKey

C、PC 端浏览器
D、PC 端浏览器与 SSL VPN 安全网关之间通信信道
答案：ACD

115. 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（ ）。
A、应用系统管理员
B、应用系统
C、密码产品
D、技术文档
答案：BC

116. 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（ ）。
A、接收到重要邮件的确认操作
B、对重要数据进行签名
C、公文管理系统业务用户公文签发操作
D、某银行网上的取钱或转账操作
答案：ABCD

450 重复
117. 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（ ）。
A、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
B、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
C、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
D、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
答案：ABCD

118. 以下选项属于设备和计算安全层面访问控制信息的是（ ）。
A、操作系统权限的访问控制信息
B、系统文件目录的访问控制信息
C、防火墙（不含密码功能）的访问控制列表
D、堡垒机中的权限访问控制信息
答案：ABD

119. 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（ ）。
A、核查安全认证网关的商用密码产品认证证书
B、核查智能密码钥匙的商用密码产品认证证书
C、通过抓包核查通信过程中的握手协议
D、通过抓包核查通信过程中的记录协议

答案：ABC

120. 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（　）。
A、查看发卡时密钥分散的密码算法
B、核查电子门禁系统的商用密码产品认证证书
C、核查门禁卡的管理制度
D、核查是否有机房进出登记记录
答案：ABC

121. 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（　）。
A、核查电子门禁系统的商用密码产品认证证书
B、核查服务器密码机的商用密码产品认证证书
C、核查是否能够修改电子门禁记录
D、核查是否能够发现修改电子门禁记录数据
答案：BCD

122. 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（　）。
A、云平台运行所在机房应作为测评对象
B、服务器密码机不作为测评对象
C、服务器密码机应作为测评对象
D、电子签章系统应作为测评对象
答案：ACD

123. 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（　）。
A、需要核查是否实现重要数据的机密性保护
B、需要核查是否实现重要数据的完整性保护
C、需要核查云服务器密码机的商用密码产品认证证书
D、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
答案：ABC

124. 密评过程中，以下属于测评实施方式的是（　）。
A、随机性检测
B、数字证书格式合规性检测
C、IPSec/SSL 协议分析
D、端口扫描
答案：ABCD

125. 密评过程中，以下能获取的数据是（　）。
A、SSL 协议通信数据
B、IPSec 协议通信数据
C、远程管理通道数据

D、密码机内的密钥数据明文
答案：ABC

126. 某证书的签名算法是 1.2.156.10197.1.501，则意味着（　）。
A、该证书所包含的公钥是 SM2 公钥
B、签发该证书采用的是 SM3withSM2Encrypt ion 算法
C、颁发者所使用的公钥是 SM2 公钥
D、不考虑编码，该证书的签名值长度应为 64 字节
答案：BCD

127. 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。
A、用户使用安全浏览器的终端
B、SSL VPN 内部
C、安全浏览器与 SSL VPN 之间的通信信道
D、信息系统所属内网的服务器
答案：ABC

128. 以下（　）方法可以用于辅助数字证书的分析。
A、对数字证书的数字签名算法进行正确性验证
B、对数字证书进行随机性检测
C、使用 ASN.1 工具对数字证书格式进行解析
D、对数字证书的杂凑密码算法进行正确性验证
答案：ACD

129. 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（　）。
A、tbsCertList
B、tbsCertificate
C、signatureAlgorithm
D、signatureValue
答案：BCD

130. 一般数字证书的后缀名是（　）。
A、cer
B、Crt
C、Der
D、Pem
答案：ABCD

131. 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（　）。
A、可接入安装有国密 SSL 安全浏览器的客户端，捕获 SSL 协议建立过程的数据包
B、一定可以查看到握手协议中双方的身份证书
C、可查看到双方协商的用于密钥协商的算法

D、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
答案：BD

132. 以下关于 Wireshark 过滤规则的说法，（ ）是正确的。
A、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
B、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
C、udp.dstport==00:11:2 2:33:44:55 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
D、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
答案：AD

133. 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（ ）。
A、盐值
B、口令明文
C、杂凑值
D、盐值与口令的组合方式
答案：ABCD

134. 一个数据的 ASN.1 编码如下：{0x02，0x12 ， ……}，那么以下说法正确的是（ ）。
A、这是一个整数（INTEGER）
B、这是一个序列（SEQUENCE）
C、其实际数据长度是 12 字节
D、其实际数据长度是 18 字节
答案：AD

135. 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（ ）。
A、这是一个序列（SEQUENCE）
B、其实际数据长度是 82 字节
C、其实际数据长度是 100 字节
D、其实际数据长度是 256 字节
答案：AD

136. 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（ ）。
A、密文长度为 192 比特
B、密文长度为 64 比特
C、IV 值以明文形式存储
D、IV 值都为全 0
答案：ABD

137. 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（ ）。
A、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）
B、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
C、检查智能密码钥匙是否具备商用密码产品认证证书
D、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
答案：ABC

138. 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（)。
A、通信双方进行加密通信前，使用双证书中的加密证书进行 SM2 密钥协商
B、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
C、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
D、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
答案：AC

139. 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（ ）。
A、可以确定使用了 SM3 对口令进行杂凑保护
B、可能采用了 MD5 对口令进行杂凑计算
C、计算口令杂凑值时可能未加入用户唯一的盐值
D、A 和 B 可能共享相同的口令
答案：CD

140. 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（ ）。
A、发送的挑战值是否每次均不重复
B、使用对应公钥能否对签名值通过验签操作
C、公钥或对称密钥与实体的绑定方式
D、对数字证书格式正确性进行验证
答案：ABCD

141. 以下关于用户密钥的存储方式， 说法正确的是（ ）。
A、数据加密密钥在经过检测认证的三级密码模块中存储
B、SM2 签名私钥经 SM4-GCM 加密后存储在数据库中
C、SM2 签名证书明文存储在应用服务器中
D、SM4 密钥经 SHA1 加密存储在数据库
答案：ABC

142. 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（ ）。
A、用户名+短信验证码
B、用户名+智能密码钥匙+PIN 码
C、人脸+指纹
D、用户名+动态令牌
答案：BD

143. 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（ ）。
A、同一个密钥既用于加密保护又用于安全认证
B、公钥明文存储在数据库中，未进行完整性保护
C、在进行签名验签前未对公钥证书有效性进行验证
D、对签名私钥进行归档
答案：ABCD

144. 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。 A、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
B、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
C、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
D、建立人员保密和调离制度，签订保密合同
答案：BCD

145. 关于数字证书的使用，以下存在风险的有（ ）。
A、证书中未标明持有者的身份
B、证书在使用前未验证真实性和有效性
C、未及时更新 CRL 或未使用 OCSP 查询证书状态
D、CA 签发的用户证书在未保护的通道中进行分发
答案：ABC

146. 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（ ）。
A、该协议使用 RSA 密码算法的数字信封功能进行密钥协商
B、该协议使用 AES-256 的 GCM 工作模式保护传输数据的机密性
C、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
D、该协议使用 AES-256 的 GCM 工作模式保护传输数据的完整性
答案：BCD

147. 以下属于存在安全问题的或安全强度不足的密码算法是（ ）。
A、MD5
B、AES128
C、RSA1024
D、SHA-1
答案：ACD

148. 随着计算机与密码技术的不断发展，部分密码算法已经无法提供安全的密码服务，以下属于存在安全问题的或安全强度不足的密码算法是（　　）。
A、 MD5
B、SHA1
C、SM1
D、 RSA4096
答案：AB

149. 下列哪些算法属于单表代换密码？（　　）
A、凯撒密码
B、放射密码
C、移位密码
D、希尔密码
答案：ABC

150. 下述哪些是哈希函数的？（　　）
A、单向性
B、输出是固定长度
C、抗原像攻击
D、抗强碰撞攻击
答案：ABCD

151. 下述哪些是数字签名算法的性质？（　　）
A、否认性
B、不可伪造性
C、保密性
D、公开可验证性
答案：BD

152. 对密码系统的攻击类型包括（　　）。
A、选择明文攻击
B、选择密文攻击
C、已知明文攻击
D、唯密文攻击
答案：ABCD

153. 国家密码管理局发布的椭圆曲线公钥密码算法（SM2 算法），在我们国家商用密码体系中不能被用来替换（　）算法。
A、DES
B、MD5
C、RSA
D、IDEA
答案：ABD

154. 身份鉴别是安全服务中的重要一环，以下关于身份鉴别叙述正确的是（　）。

A、目前一般采用基于对称密钥加密或公开密钥加密的方法
B、身份鉴别一般不用提供双向的认证
C、数字签名机制是实现身份鉴别的重要机制
D、身份鉴别是授权控制的基础
答案：ACD

155. 下述关于密码学论述的观点正确的是（　　）。
A、密码学的属性包括机密性、完整性、真实性、不可否认性
B、密码学的两大分支是密码编码学和密码分析学
C、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
D、密码技术并不是提供安全的唯一手段
答案：ABCD

156. 属于密码在信息安全领域的具体应用的是（　　）。
A、生成所有网络协议
B、消息鉴别，确保信息完整性和真实性
C、加密保护，保护传输信息的机密性
D、身份鉴别
答案：BCD

157. ZUC 算法中，比特重组（BR）过程从 LFSR 中抽取哪些寄存器单元来构造 X0、X1、X2、X3？（　）
A. s15, s14
B. s11, s9
C. s7, s5
D. s2, s0
答案：ABD

158. 以下属于现代密码学范畴的是（　　）。
A、DES
B、Vigenere
C、Caesar
D、RSA
答案：AD

三、判断题 80
1.某公司上线了协同签名系统，该系统为了实现效率，使用了 ZUC 算法实现数字签名。
答案：错

2.5G 空口加密中，使用 ZUC 算法时可以将基站小区 ID 作为固定 IV 以提高效率。
答案：错

3.将 ZUC 算法的密钥长度扩展到 256 位（ZUC-256）即可抵抗量子计算机的暴力破解。
答案：错

4.一般来说，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。
答案：对

5.在密码学中，需要被变换的原消息被称为密文。
答案：错

6.古典密码体制中，移位密码属于置换密码。
答案：错

7.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。答案：对

8.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。
答案：对

9.商用密码用于保护属于国家秘密的信息。
答案：错

10.“一次一密”的随机密码序列体制在理论上是不可破译的。
答案：对

11.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。
答案：对

12.所有的线性变换都能成为一个有效的仿射加密函数。
答案：错

13.置换（permutation）密码采用线性变换对明文进行处理。
答案：对

14.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。
答案：对

15.古典 Vigenere 密码是一个单表代换密码。
答案：错

16.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行代换的密码。答案：对

17.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。
答案：对

18.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。
答案：对

19.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。
答案：错

20.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。
答案：对

21.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。
答案：错

22.ZUC 算法是一个序列密码算法。
答案：对

23.ZUC 算法是中国自主设计的密码算法。
答案：对

24.ZUC 算法是一个基于字设计的序列密码算法。
答案：对

25.SM3 密码杂凑算法和 SHA-256 的压缩函数完全相同。
答案：错

26.SHA-512 的输出长度是 512 比特。
答案：对

27.SHA-512 以 512 位的分组为单位处理消息。
答案：错

28.SHA-512 处理消息时，每个分组有 80 轮运算。
答案：对

29.SM9 是基于标识的密码算法。
答案：对

30.SM2 签名速率一般小于验签速率。
答案：错

31.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。
答案：对

32.SM2 算法的安全性是基于因子分解困难问题。

答案：错

33.SM2 算法的安全性是基于椭圆曲线离散对数问题。
答案：对

34.SM2 数字签名算法已经入选 ISO 国际标准。
答案：对

35.SM2 加密算法可以用来保护消息机密性。
答案：对

36.SM2 算法与国际 ECDSA 算法采用了部分类似的数学结构。
答案：对

37.SM2 算法是对称加密算法。
答案：错

38.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。
答案：错

39.远程人脸识别系统应具备对人脸数据进行备份的能力以及相应的恢复控制措施。
答案：对

40.我国被采纳为新一代宽带无线移动通信系统（LTE）国际标准的算法是 SM2 算法。
答案：错

41.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。
答案：对

42.置换密码又叫换位密码，常见的置换密码有栅栏密码等。
答案：对

43.现代密码学中，为了保证安全性，密码算法应该进行保密。
答案：错

44.SM2、SM4、ZUC 算法都是对称密码算法。
答案：错

45.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。
答案：错

46.最短向量问题是格上的困难问题。

答案：对

47.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。
答案：对

48.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。
答案：对

49.多表代换密码是以单个代换表对多组明文进行加密。
答案：错

50.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。
答案：对

51.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。
答案：对

52.SM3 密码杂凑算法中的 P 置换是非线性运算。
答案：错

53.SM3 密码杂凑算法一共有 2 个置换函数。
答案：对

54.SM3 密码杂凑算法的消息扩展过程一共生成 128 个消息字。
答案：错

55.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。
答案：对

56.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。
答案：对

57.SM9 密钥交换协议要求必须有密钥确认。
答案：错

58.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。
答案：错

59.SM9 密码算法用户标识由 KGC 生成。
答案：错

60.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。

答案：对

61.SM9 密码算法系统参数由 KGC 选择。
答案：对

62.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。
答案：错

63.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。
答案：对

64.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。
答案：对

65.基于口令（PASSWORD）的密钥派生函数需要调用密码杂凑函数。
答案：错

66.SM9 标识密码算法密钥交换过程中不需要计算群中的元素。
答案：错

67.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。
答案：对

68.在公钥加密算法中，私钥用于加密消息，公钥用于解密消息。
答案：错

69.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。
答案：对

70.维吉尼亚密码属于单表代换密码。
答案：错

71.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。
答案：对

72.OFB 加密模式在解密过程中需要执行分组密码的解密操作。
答案：错

73.CBC 加密模式在解密过程中需要执行分组密码的解密操作。
答案：对

74.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。
答案：对

75.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。
答案：错

76.CCM 不仅能加密数据，还能够保护数据的完整性。
答案：对

77.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。
答案：对

78.ZUC 算法 LFSR 部分产生的二元序列具有很低的线性复杂度。
答案：对

79.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。
答案：对

80.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。
答案：对

二、信息安全 120

一、单选题 80
1. 近年来，移动终端普遍集成指纹、面部和虹膜识别技术，以提升身份验证的安全性和便捷性。下列相关描述中，哪一项是错误的？（ ）
A、指纹识别可能被高精度模具复制
B、面部识别在弱光环境下准确性下降
C、虹膜识别安全性高于传统口令
D、生物信息泄露后可通过修改口令重置
答案：D

2. 在节能环保、安全舒适，以及车联网、自动驾驶、智能交通等方面的推动下，汽车正在迅速智能化、网联化，车联网网络安全对交通安全、社会安全和国家安全具有重要影响。关于车联网网络安全，描述错误的是（ ）。
A、车内单元的安全能力，受限于设备体积、成本、存储空间和计算能力，需要研究与其相匹配的轻量级安全解决方案
B、车联网包括移动互联网络和车内工控网络
C、车与车之间的直接连接，尽管距离很近，也必须考虑安全连接问题
D、车联网也是一种互联网，可以采用与目前互联网一样的安全防护技术手段
答案：D

3. 近年来，不法分子利用黑客技术破解并控制家用及公共场所摄像头，将智能手机、运动手环等改装成偷拍设备，形成黑产链条，严重侵害公民个人隐私。以

下在全国摄像头偷窥黑产集中治理过程中，相关职责描述错误的是（　　）。
A. 社交软件、网站、论坛等互联网平台要严格履行信息发布审核的主体责任
B. 摄像头生产企业要全面开展排查，对平台上的假冒伪劣摄像头做下架处理
C. 公安机关依法打击获取买卖公民隐私视频等违法犯罪活动
D. 网信、工信、市场监管等部门加强监管和执法
答案：A

4. 可信计算（Trusted Computing）是一种通过硬件和软件结合来增强系统安全性的技术，但它也可能面临多种网络安全威胁。以下哪些是可信计算可能面临的网络安全威胁？（　）
A、TPM 芯片的物理侧信道攻击
B、恶意软件篡改 PCR 值
C、远程证明过程中的中间人攻击
D、DDoS 攻击
答案：ABC

5. 单位使用公有云存储敏感文件时，为确保数据在传输和静态存储中的安全性，应采取的最核心措施是（　）。
A、启用多因素认证（MFA）
B、使用 SSL/TLS 加密传输并配置服务端加密（SSE）
C、定期更新防火墙规则
D、限制 API 调用频率
答案：B

6. 在物联网领域中，安全威胁和攻击类型多种多样，每种攻击都有其特定的防护措施。请将左侧的物联网攻击类型与右侧对应的防护措施正确连线：

攻击类型	防护措施
1. DDoS 攻击	A. 强制使用强口令策略
2. 中间人攻击	B. 部署流量清洗系统
3. 固件漏洞利用	C. 定期更新设备固件
4. 弱口令爆破	D. 启用端到端加密通信

A、1—B；2—D；3—C；4—A
B、1—C；2—A；3—B；4—D
C、1—A；2—B；3—D；4—C
D、1—D；2—C；3—A；4—B
答案：A

7. 流量分析工具的用途是（　　）。
A、主要是从系统日志中读取出曾发生的安全事件，以此降低人工审计的工作量
B、主要是对网络流量进行分析，从中发现异常访问行为
C、可以自动阻断攻击或入侵
D、主要是对入侵、攻击、非法访问等行为检测
答案：B

8. 下列关于信息安全策略维护的说法，（　　）是错误的。

A、安全策略的维护应当由专门的部门完成
B、安全策略制定完成并发布之后，不需要再对其进行修改
C、应当定期对安全策略进行审查和修订
D、维护工作应当周期性进行
答案：B

9. 在可信计算中，可信平台模块（TPM）是一个专用的微控制器，旨在通过提供硬件级别的安全来增强设备的安全性。下面列出了几个关于 TPM 功能的选项，请根据对 TPM 的理解选择最准确描述其核心功能的一项。（ ）
A、加密硬盘中的所有数据
B、提供硬件级密钥管理和安全存储
C、阻止网络钓鱼攻击
D、提升系统运行速度
答案：B

10. 某网站允许用户上传任意文件，攻击者上传了一个包含恶意代码的.php 文件并通过 URL 直接访问执行。此漏洞最可能的原因是（ ）。
A、未启用 HTTPS 协议
B、未对文件扩展名和内容进行双重校验
C、未设置 CSP（内容安全策略）
D、未使用验证码（CAPTCHA）
答案：B

11. 在工控系统网络架构中，典型的分层结构主要基于功能分区和安全需求，而非传统企业网络的物理拓扑分层。那么，以下哪项是工控系统网络架构典型的分层结构？（ ）
A、核心层、汇聚层、接入层
B、控制网、数据采集网、办公网
C、物理层、数据链路层、应用层
D、服务器层、客户端层、存储层
答案：B

12. 无线传感器网络容易受到各种恶意攻击，以下关于其防御手段说法错误的是（ ）。
A、采用干扰区内节点切换频率的方式抵御干扰
B、通过向独立多路径发送验证数据来发现异常节点
C、利用中心节点监视网络中其它所有节点来发现恶意节点
D、利用安全并具有弹性的时间同步协议对抗外部攻击和被俘获节点的影响
答案：C

13. 关于网络安全服务的叙述中，（ ）是错误的。
A、应提供信息重传服务以防止用户否认已接收的信息
B、应提供认证服务以保证用户身份的真实性
C、应提供数据完整性校验服务以防止信息在传输过程中被删除
D、应提供数据加解密服务以防止传输的数据被截获或篡改
答案：A

14. 以下不属于网络安全控制技术的是（　　）。
A、防火墙技术
B、访问控制技术
C、入侵检测技术
D、流量限定技术
答案：D

15. （　　）不仅是实现网络通信的主要设备之一，而且也是关系全网安全的设备之一，它的安全性、健壮性将直接影响网络的可用性。
A、 网闸
B、日志审计系统
C、路由器
D、入侵防御系统
答案：C

16. 网站是对外服务的窗口，其安全性日益受到关注。目前，网站面临多个方面的安全威胁。“攻击者通过口令猜测及“撞库”攻击技术手段，获取网站用户的访问权限”属于（　　）。
A、网页篡改
B、非授权访问
C、恶意代码
D、数据泄露
答案：B

17. 网络安全漏洞管理包含漏洞发现和报告、漏洞接收、漏洞验证、漏洞处置、漏洞发布、漏洞跟踪等阶段，那么对漏洞进行修复是属于（　　）。
A、漏洞发现和报告
B、漏洞验证
C、漏洞处置
D、漏洞跟踪
答案：C

18. 下列对于 DMZ 区的说法错误的是（　　）。
A、它是网络安全防护的一个“非军事区”
B、它是对“深度防御”概念的一种实现方案
C、它是一种比较常用的网络安全域划分方式
D、它是互联网服务运行的必备条件
答案：D

19. 大数据时代，人类就像生活在“玻璃房”里，道出了大数据时代潜在的安全风险。“通过关联分析用户在社交网站中写入的信息、智能手机显示的位置信息等多种数据，识别到自然人，挖掘出个人信息”属于（　　）。
A、数据共享存在的敏感信息泄露风险
B、数据不准确带来的利益风险
C、大数据恶意使用给个人信息保护带来的安全风险

D、数据汇聚增加的易遭受网络攻击的风险
答案：C

20. 对日志服务器进行分析时，发现某一时间段，网络中有大量包含“USER”、“PASS”负载的数据，该异常行为最可能是（　　）。
A、ICMP 泛洪攻击
B、端口扫描
C、弱口令扫描
D、TCP 泛洪攻击
答案：C

21. 信息安全风险评估是一个技术过程，更是一种战略性的管理活动，能够帮助组织识别和应对潜在的安全威胁，优化资源配置，提升业务连续性和弹性。其中，信息安全风险评估的核心环节是（　　）。
A、资产识别
B、威胁识别
C、脆弱性识别
D、已有安全措施识别
答案：A

22. 关键信息基础设施发生重大网络安全事件或者发现重大网络安全威胁时，运营者应当按照有关规定向保护工作部门、（　　）报告。
A、网信部门
B、公安机关
C、电信部门
D、网安部门
答案：B

23. 深度流检测技术是一种主要通过判断网络流是否异常来进行安全防护的网络安全技术，深度流检测系统通常不包括（　　）。
A、流特征提取单元
B、流特征选择单元
C、分类器
D、响应单元
答案：D

24. 在信息安全和隐私保护领域，隐私可以根据其性质分为多个类别，包括身份隐私、属性隐私、社交关系隐私、位置轨迹隐私等大类，那么，员工的薪资收入属于哪一类隐私?（　　）
A、身份隐私
B、属性隐私
C、社交关系隐私
D、位置轨迹隐私
答案：B

25. 日常安全运维管理中，服务器管理员会使用（　　）来安全连接远程服务器。

A、Telnet
B、安全文件传输协议（SFTP）
C、安全拷贝（SCP）
D、安全外壳（SSH）
答案：D

26. 国家保护个人、组织与数据有关的权益，鼓励数据依法合理有效利用，保障数据依法有序自由流动，促进以（　　）为关键要素的数字经济发展。
A、数据
B、信息
C、创新能力
D、硬核科技
答案：A

27. 某公司的员工，正当他在忙于一个紧急工作时，接到一个电话，被告知系统发现严重漏洞，紧急修复，需提供他的系统管理账户信息，接下来他的正确做法是（　　）
A、核实之后，如是真实情况，才可提供账号信息
B、诈骗电话，直接挂机
C、直接拒绝
D、报警
答案：A

28. 打开一份邮件时，处理邮件附件的正确做法是（　　）
A、确认发件人信息真实后，查杀病毒后打开
B、置之不理
C、删除附件
D、直接打开运行
答案：A

29. 网络关键设备和网络安全专用产品应当按照相关国家标准的强制性要求，由具备资格的机构（　　）或者安全检测符合要求后，方可销售或者提供。
A、鉴定产品功能
B、安全认证合格
C、测试产品性能
D、认证产品质量合格
答案：B

30. SQL 是一种数据库结构化查询语言，其中 SQL 注入攻击的首要目标是(　　)。
A、破坏 Web 服务
B、窃取用户口令等机密信息
C、攻击用户浏览器，以获得访问权限
D、获得数据库的权限
答案：D

31. 规范的实施流程和文档管理，是信息安全风险评估能否取得成果的重要基

础，按照规范的风险评估实施流程，下面哪个文档应当是风险要素识别阶段的输出成果？（　）
A、《风险评估方案》
B、《需要保护的资产清单》
C、《风险计算报告》
D、《风险程度等级列表》
答案：B

32. 在软件保障成熟度模型（SAMM) 中，规定了软件开发过程中的核心业务功能，下列哪个选项不属于核心业务功能？（　）
A、治理，主要是管理软件开发的过程和活动
B、构造，主要是在开发项目中确定目标并开发软件的过程与活动
C、验证，主要是测试和验证软件的过程和活动
D、购置，主要是购买第三方商业软件或者采用开源组件的相关管理过程与活动
答案：D

33. 用户收到了一封陌生人的电子邮件，提供了一个 DOC 格式的附件，用户有可能会受到（　）。
A. 溢出攻击
B. 目录遍历攻击
C. 后门攻击
D. DDOS
答案：A

34. 下面有关软件安全问题的描述中，哪项是由于软件设计缺陷引起的（　）。
A、设计了三层 We b 架构，但是软件存在 SQL 注入漏洞，导致被黑客攻击后能直接访问数据库
B、使用 C 语言开发时，采用了一些存在安全问题的字符串处理函数，导致存在缓冲区溢出漏洞
C、设计了缓存用户隐私数据机制以加快系统处理性能，导致软件在发布运行后，被黑客攻击获取用户隐私数据
D、使用了符合要求的密码算法，但在使用算法接口时，没有按照要求生成密钥，导致黑客攻击后能破解并得到明文数据
答案：C

35. 某集团公司根据业务需求，在各地分支机构部署前置机，为了保证安全，集团总部要求前置机开放日志共享，由总部 服务器采集进行集中分析，在运行过程中发现攻击者也可通过共享从前置机种提取日志，从而导致部分敏感信息泄露，根据降低攻击面的原则，应采取以下哪项处理措施（　）。
A、由于共享导致了安全问题，应直接关闭日志共享，禁止总部提取日志进行分析
B、为配合总部的安全策略，会带来一定安全问题，但不影响系统使用，因此接受此风险
C、日志的存在就是安全风险，最好的办法就是取消日志，通过设置前置机不记录日志
D、只允许特定 IP 地址从前置机提取日志，对日志共享设置访问密码且限定访

问的时间
答案：D

36. 对软件的拒绝服务攻击是通过消耗系统资源使软件无法响应正常请求的一种攻击方式，在软件开发时分析拒绝服务 攻击的威胁，以下哪个不是需求考虑的攻击方式（　　）。
A、攻击者利用软件存在的逻辑错误，通过发送某种类型数据导致运算进入死循环，CPU 资源占用始终 100%
B、攻击者利用软件脚本使用多重嵌套咨询，在数据量大时会导致查询效率低，通过发送大量的查询导致数据库响应缓慢
C、攻击者利用软件不自动释放连接的问题，通过发送大量连接消耗软件并发连接数，导致并发连接数耗尽而无法访问
D、攻击者买通 IDC 人员，将某软件运行服务器的网线拔掉导致无法访问
答案：D

37. 某网站为了开发的便利，使用 SA 链接数据库，由于网站脚本中被发现存在 SQL 注入漏洞，导致攻击者利用内置存 储过程 XP.cmctstell 删除了系统中的一个重要文件，在进行问题分析时，作为安全专家，你应该指出该网站设计违反了以下哪项原则（　　）。
A、权限分离原则
B、最小特权原则
C、保护最薄弱环节的原则
D、纵深防御的原则
答案：B

38. 关于信息安全管理，下面理解片面的是（　　）。
A、信息安全管理是组织整体管理的重要、固有组成部分，它是组织实现其业务目标的重要保障
B、信息安全管理是一个不断演进、循环发展的动态过程，不是一成不变的
C、信息安全建设中，技术是基础，管理是拔高，即有效的管理依赖于良好的技术基础
D、坚持管理与技术并重的原则，是我国加强信息安全保障工作的主要原则之一
答案：C

39. 降低风险（或减低风险）指通过对面的风险的资产采取保护措施的方式来降低风险，下面哪个措施不属于降低风险的措施？（　　）
A、减少威胁源，采用法律的手段制裁计算机的犯罪，发挥法律的威慑作用，从而有效遏制威胁源的动机
B、签订外包服务合同，将有计算难点，存在实现风险的任务通过签订外部合同的方式交予第三方公司完成，通过合同责任条款来应对风险
C、减低威胁能力，采取身份认证措施，从而抵制身份假冒这种威胁行为的能力
D、减少脆弱性，及时给系统打补丁，关闭无用的网络服务端口，从而减少系统的脆弱性，降低被利用的可能性
答案：B

40. 关于风险要素识别阶段工作内容叙述错误的是（　　）。

A、资产识别是指对需求保护的资产和系统等进行识别和分类
B、威胁识别是指识别与每项资产相关的可能威胁和漏洞及其发生的可能性
C、脆弱性识别以资产为核心，针对每一项需求保护的资产，识别可能被威胁利用的弱点，并对脆弱性的严重程度进行评估
D、确认已有的安全措施仅属于技术层面的工作，牵涉到具体方面包括：物理平台、系统平台、网络平台和应用平台
答案：D

41. 某单位的信息安全主管部门在学习我国有关信息安全的政策和文件后，认识到信息安全风险评估分为自评估和检查评估两种形式，该部门将检查评估的特点和要求整理成如下四条报告给单位领导，其中描述错误的是（　　）。
A、检查评估可依据相关标准的要求，实施完整的风险评估过程；也可在自评估的基础上，对关键环节或重点内容实施抽样评估
B、检查评估可以由上级管理部门组织，也可以由本级单位发起，其重点是针对存在的问题进行检查和评测
C、检查评估可以由上级管理部门组织，并委托有资质的第三方技术机构实施
D、检查评估是通过行政手段加强信息安全管理的重要措施，具有强制性的特点
答案：B

42. 在信息安全管理的实施过程中，管理者的作用于信息安全管理体系能否成功实施非常重要，但是以下选项中不属于管理者应有职责的是（　　）。
A、制定并颁发信息安全方针，为组织的信息安全管理体系建设指明方向并提供总体纲领，明确总体要求
B、确保组织的信息安全管理体系目标和相应的计划得以制定，目标应明确、可度量，计划应具体、可实施
C、向组织传达满足信息安全的重要性，传达满足信息安全要求、达成信息安全目标、符合信息安全方针、履行法律 责任和持续改进的重要性
D、建立健全信息安全制度，明确安全风险管理作用，实施信息安全风险评估过程、确保信息安全风险评估技术选择 合理、计算正确
答案：D

43. 信息安全管理体系（ISMS）的内部审核和管理审核是两项重要的管理活动，关于这两者，下面描述的错误是（　　）。
A、内部审核和管理评审都很重要，都是促进 ISMS 持续改进的重要动力，也都应当按照一定的周期实施
B、内部审核实施方式多采用文件审核和现场审核的形式，而管理评审的实施方式多采用召开管理评审会议形式进行
C、内部审核实施主体组织内部的 ISMS 内审小组，而管理评审的实施主体是由国家政策指定的第三方技术服务机构
D、组织的信息安全方针、信息安全目标和有关 ISMS 文件等，在内部审核中作为审核标准使用，但在管理评审中，这些文件是被审对象
答案：C

44. 在风险管理中，残余风险是指实施了新的或增强的安全措施后还剩下的风险，关于残余风险，下面描述错误的是（　　）。
A、风险处理措施确定以后，应编制详细的残余风险清单，并获得管理层对残余

风险的书面批准，这也是风险管理中 的一个重要过程
B、管理层确认接收残余风险，是对风险评估工作的一种肯定，表示管理层已经全面了解了组织所面临的风险，并理解在风险一旦变为现实后，组织能够且承担引发的后果
C、接收残余风险，则表明没有必要防范和加固所有的安全漏洞，也没有必要无限制的提高安全保护措施的强度，对 安全保护措施的选择要考虑到成本和技术等因素的限制
D、如果残余风险没有降低到可接受的级别，则只能被动的选择接受风险，即对风险不进行下一步的处理措施，接受 风险可能带来的结果。
答案：D

45. 关于业务连续性计划（BCP）以下说法最恰当的是（ ）。
A、组织为避免所有业务功能因重大事件而中断，减少业务风险而建立的一个控制过程。
B、组织为避免关键业务功能因重大事件而中断，减少业务风险而建立的一个控制过程。
C、组织为避免所有业务功能因各种事件而中断，减少业务风险而建立的一个控制过程
D、组织为避免信息系统功能因各种事件而中断，减少信息系统风险建立的一个控制过程
答案：B

46. ISMS 是组织的一项战略性决策，其设计和实施受需要、目标、安全要求、所采用的过程以及组织的规模和结构影响。ISMS 是指（ ）。
A、信息安全管理体系
B、信息服务管理体系
C、信息技术管理体系
D、信息产品管理体系
答案：A

47. 检查云计算管理平台的网络安全时，需检查虚拟网络边界的（ ）策略，查看其是否对进出网络的信息内容进行过滤，实现对应用层 HTTP、FTP、TELNET、SMTP、POP3 等的控制。
A、访问控制
B、属性安全控制
C、目录级安全控制
D、网络锁定控制
答案：A

48. 机房建设是一个系统工程，要切实做到从工作需要出发，以人为本，满足功能需求，能够为设备提供一个安全运行的空间。以下场地中，适宜机房建设的是（ ）。
A、建筑物顶楼
B、建筑物的地下室
C、建筑物的中间楼层
D、盥洗室的隔壁房间

答案：C

49. 当前，网络直播行业存在的主体责任缺失、内容生态不良等问题，严重制约网络直播行业健康发展。各部门应当切实履行职能职责，依法依规加强对网络直播行业相关业务的监督管理。（　　）要进一步强化网络直播行业管理的统筹协调和日常监管。
A、工业和信息化部门
B、市场监督管理部门
C、网信部门
D、行政执法部门
答案：C

50. 系统调用是用户在程序中调用操作系统所提供的一些子功能，系统调用可以被当作特殊的公共子程序。下面关于系统调用的描述中，错误的是（　）。
A、系统调用中被调用的过程运行在“用户态”中
B、利用系统调用能够得到操作系统提供的多种服务
C、系统调用把应用程序的请求传输给系统内核执行
D、系统调用保护了一些只能在内核模式执行的操作指令
答案：A

51. 不属于计算机病毒防治策略的是（　）。
A、及时安装操作系统补丁
B、及时、可靠升级防病毒产品
C、对新购置的计算机软件进行病毒检测
D、定期整理磁盘
答案：D

52. 光盘被划伤，无法读取数据，是破坏了载体的（　）。
A、机密性
B、完整性
C、可用性
D、真实性
答案：C

53. 单位网络管理员小李发现局域网中有若干台电脑有感染病毒的迹象，这时应首先（　），以避免病毒的进一步扩散。
A、关闭服务器
B、启动反病毒软件查杀
C、断开有嫌疑计算机的物理网络连接
D、关闭网络交换机
答案：C

54. 以下有关云计算的表达，不恰当的是（　）。
A、云计算是一种按使用量付费的模式
B、这种模式提供可用的、便捷的、按需的网络访问
C、云计算的可配置计算资源共享池包括网络、服务器、存储、应用软件、服务

等资源
D、云计算服务是通过卫星进行的数据服务
答案：D

55. 在某次信息安全应急响应过程中，小王正在实施如下措施：消除或阻断攻击源，找到并消除系统的脆弱性/漏洞、修改安全策略，加强防范措施、格式化被感染而已程序的介质等，请问按照应急响应方法，这些工作应处于以下哪个阶段（　　）。
A、准备阶段
B、检测阶段
C、遏制阶段
D、根除阶段
答案：D

56. 网络信息安全基本属性包括：机密性、完整性、可用性、抗抵赖性和可控性等。其中网络信息不泄露给非授权用户、实体或程序，能够防止未授权者获取网络信息是指（　　）。
A、机密性
B、完整性
C、可用性
D、可控性
答案：A

57. 风险管理是一个系统的过程，旨在识别、评估和控制可能影响企业目标实现的不确定性和潜在威胁。风险管理的最佳战略是（　　）。
A、实现风险与组织目的之间的平衡
B、将风险降至可接受水平
C、确保政策的制定正确考虑了组织风险
D、确保管理层接受所有未经缓解的风险
答案：B

58. 信息系统受到破坏后，会对社会秩序和公共利益造成严重损害，或者对国家安全造成损害，按照计算机信息系统安全等级保护相关要求，应定义为（　　）。
A、第一级
B、第二级
C、第三级
D、第四级
答案：C

59. 数字水印技术是一种用于在多媒体数据中嵌入特定信息的技术，可以根据其功能、特性和应用领域进行分类。通常用于数字化图像、视频、音频或电子文档的版权保护的是（　　）。
A、鲁棒水印
B、易损水印
C、标注水印
D、动态水印

答案：A

60. 为保护移动应用（App）的安全性，通常采用防反编译、防调试、防篡改和防窃取等多种安全保护措施。其中，将类名、方法名和变量名替换为无意义的简短名称，有效对抗逆向工程的技术属于（　　）。
A、防反编译
B、防调试
C、防篡改
D、防窃取
答案：A

61. 为了有效防范网络安全漏洞，多种技术被开发和应用，常见的网络安全漏洞利用防范技术主要有地址空间随机化技术、数据执行阻止、堆栈保护、虚拟补丁等。那么，Web 应用防火墙属于（　　）。
A、地址空间随机化技术
B、数据执行阻止
C、堆栈保护
D、虚拟补丁
答案：D

62. 构建云计算安全等级保护框架时，遵循“一个中心，三重防护”的原则是关键。其中一个中心是指安全管理中心，三重防护为计算环境安全、区域边界安全和通信网络安全。以下安全机制属于计算环境安全的是（　　）。
A、安全事件监测
B、应用安全
C、网络隔离
D、抗 DDoS 攻击
答案：B

63. 网络信息安全基本属性包括：机密性、完整性、可用性、抗抵赖性和可控性等。其中网络信息不泄露给非授权用户、实体或程序，能够防止未授权者获取网络信息是指（　　）。
A、机密性
B、完整性
C、可用性
D、可控性
答案：A

64. 在路由器配置时，使用（　　）命令可以将口令以加密（密文）的形式保存，在网络设备配置中这是常用的一种安全措施，确保即使配置文件被未经授权的人员查看，口令也不会轻易暴露。
A、enable secret
B、secure boot-image
C、login local
D、crypto key generate
答案：A

65. 依据 GB/T 20984-2022《信息安全技术 信息安全风险评估方法》，在（　　）阶段，要持续的实施风险评估以识别评估对象面临的不断变化的风险和脆弱性，从而确定安全措施的有效性，确保安全目标得以实现。
A、规划设计
B、实施交付
C、运行维护
D、建设验收
答案：C

66. 中标麒麟可信操作系统结构包括管理子系统、安全子系统、可信子系统和应用开发环境四个部分，其中身份鉴别功能属于系统安全的重要组成部分，主要用于验证用户或系统的身份，属于（　　）。
A、管理子系统
B、应用开发环境
C、可信子系统
D、安全子系统
答案：D

67. 计算机病毒通常附加在正常软件或文档中，一旦触发执行，就会潜入受害用户的计算机。以下计算机病毒以 Word 文档为隐蔽载体是（　　）。
A、CIH 病毒
B、Nimda 病毒
C、Melissa 病毒
D、Sasser 病毒
答案：C

68. ARP 病毒利用了 ARP 协议本身的弱点，通过（　　），对网络通信安全构成了严重威胁。
A、SYN 泛红占用大量网络带宽导致网络拥塞
B、加密网络流量使其无法被正常解析
C、拦截和篡改 IP 数据包
D、伪造 ARP 请求或应答来欺骗网络中的设备
答案：D

69. 在 TCP/IP 模型中，由 OSI/RM（开放系统互联参考模型）表示层定义的数据压缩、加密等功能实际上是由（　　）来实现的。
A、物理层
B、网络层
C、传输层
D、应用层
答案：D

70. 在量子通信领域，为了实现信息的绝对安全传输，通常采用（　　）。
A、量子隐形状态，无需物理介质，通过量子纠缠实现
B、单个光子，通过超低损耗的单模光纤传输

C、经典电磁波，通过光纤传输
D、纠缠态量子比特，通过自由空间(如大气层)传输
答案：A

71. 远程桌面连接的应用非常广泛，几乎涵盖了所有需要远程访问计算机资源的场景。在远程桌面连接中，通常使用（　　）协议来保护数据传输的安全性。
A、FTP
B、HTTP
C、SSL/TLS
D、SFTP
答案：C

72. 网络监控工具对于确保组织网络的稳定性、安全性和高效性至关重要。以下哪一项是网络监控工具在网络故障管理中的作用？（　　）
A、预防网络攻击
B、自动修复网络故障
C、限制网络流量
D、检测和报告网络问题
答案：D

73. 在网络安全体系模型 WPDRRC（预警、防护、检测、响应、恢复、反击）中，（　　）使用的技术包括安全套接层（SSL）流量分析、日志分析和审计等。
A、预警
B、防护
C、检测
D、响应
答案：C

74. 大数据技术架构主要包含大数据获取技术、分布式数据处理技术和大数据管理技术，以及大数据应用和服务技术。那么，（　　）主要关注大数据存储、大数据协同和安全隐私等方面。
A、大数据获取技术
B、分布式数据处理技术
C、大数据管理技术
D、大数据应用和服务技术
答案：C

75. 在由安全机制、OSI 网络参考模型、安全服务三个轴构成的信息安全系统三维空间中，安全机制轴涵盖了用于实现信息安全的各种技术手段和方法，包括基础设施安全、平台安全、数据安全、应用安全等，其中操作系统漏洞检测与修复属于（　　）。
A、基础设施安全
B、平台安全
C、数据安全
D、应用安全
答案：B

76. WEB 安全防护是一个多层次的过程，涉及从输入验证、身份验证、会话管理到数据加密等多个方面的技术措施。以下哪项不属于 WEB 安全的基本防护措施？（　　）
A、定期进行安全测试和审计
B、定期更新和修补第三方库和框架
C、使用强口令策略并定期更换口令
D、提高服务器硬件性能
答案：D

77. 可信计算的安全机制旨在通过硬件和软件的结合，提供一个安全的基础环境，确保计算机系统的安全性、数据的完整性和用户的隐私。以下关于可信计算的安全机制的描述，正确的是（　　）。
A、可信计算可增强身份验证和攻击防御能力，但对物联网设备的安全性没有帮助
B、可信计算的安全机制主要依赖于软件实现，硬件部分并不重要
C、可信计算的安全机制包括高速固态硬盘，以提高数据读写速度和安全性
D、平台配置寄存器用于存储系统组件的完整性度量值，便于后续验证系统状态
答案：D

78. 可信计算是一种通过硬件和软件结合来提高计算机系统安全性的方法，旨在解决传统计算环境中存在的安全问题，如身份验证不足等。以下（　　）属于其核心组成部分。
A、TPM (Trusted Platform Module)
B、BIOS (Basic Input/Output System)
C、CPU (Central Processing Unit)
D、GPU (Graphics Processing Unit)
答案：A

79. 在对信息安全风险进行分析和评估之后，还必须思考如何应对风险，应对风险的方式通常可分为风险规避、风险降低、风险转移、风险持有四种方式，以下方式属于风险转移的是（　　）。
A、安装杀毒软件
B、决定接受由于使用老旧但稳定的系统而带来的潜在安全威胁
C、购买网络安全保险以覆盖数据泄露的潜在损失
D、停止使用某项存在高安全风险的技术或服务
答案：C

80. 在信息安全中，对信息资产产生不利影响的因素被称为威胁，以下关于威胁的说法，错误的是（　　）。
A、错误发送了电子邮件，或丢失了 USB 存储器等情形属于故意威胁
B、地震、火灾、洪水等灾难属于环境性威胁
C、人为错误和灾难的威胁永远不会消失
D、计算机病毒和恶意软件属于技术性威胁
答案：A

二、多选题 30

1. Android 是一个开源的移动终端操作系统，共分成 Linux 内核层、系统运行库层、应用程序框架层和应用程序层四个部分。那么以下属于应用程序层的是（　　）。

A、浏览器

B、资源管理器

C、显示驱动

D、主屏

答案：AD

2. 网络信息安全事件可以根据其性质和影响范围分为多个类别，包括恶意程序事件、网络攻击事件、信息内容安全事件等。以下网络安全事件中属于信息内容安全事件的是（　　）。

A. 有意或无意地删除重要数据，导致业务中断或损失

B. 制造和散布虚假新闻或谣言，误导公众舆论

C. 通过网络传播法律法规禁止的信息，炒作敏感问题

D. 员工或合作伙伴违反公司政策，泄露敏感信息或滥用权限

答案：BC

3. “互联网+”时代，足不出户即可享受美食、打车不再需要路边招手.....，各类 App 的出现改变了人们生活的同时也带来了安全隐患。对于“餐饮外卖类 App”，以下（　　）是不属于该类 App 所规定收集的必要个人信息。

A、收货人真实姓名

B、注册用户移动电话号码

C、收货人性别

D、收货人详细门牌号码

答案：ACD

4. 网络安全漏洞是网络安全管理工作的重要内容，网络信息系统的漏洞主要来自两个方面：非技术性安全漏洞和技术性安全漏洞。以下属于非技术性安全漏洞主要来源的是（　　）。

A、网络安全责任主体不明确

B、配置错误

C、缓冲区溢出

D、网络安全监督缺失

答案：AD

5. 网络信息系统的可靠性测度主要关注的是系统在特定条件和时间段内能够无故障并正确执行其功能的能力，包括（　　）等。

A、容错性

B、生存性

C、完整性

D、有效性

答案：ABD

6. 5G 网络作为第五代移动通信技术，带来了许多新的特性和改进。以下关于

5G 网络的描述，正确的是（　　）。
A、5G 网络能够提供比 4G 快 10 到 100 倍的数据传输速率
B、5G 显著降低了数据传输的延迟时间，最低可至 1 毫秒
C、5G 支持每平方公里内多达 100 万台设备的连接
D、5G 基站的覆盖范围较大，尤其是在使用高频段时，信号穿透力强
答案：ABC

7. 某医院需保护患者隐私数据，以下哪些措施属于数据安全中的“数据脱敏”和“数据备份”技术？（　）
A、将患者姓名替换为随机生成的假名（静态脱敏）
B、每周执行差异备份并存储于异地机房
C、在查询时实时隐藏患者身份证号后四位（动态脱敏）
D、使用 RAID 1 技术实现磁盘镜像
答案：ABC

8. 某单位服务器遭受入侵后，取证人员首先对内存进行镜像备份，随后提取防火墙日志，最后将关键数据包存入写保护设备。此流程主要违反了（　）？
A、证据完整性原则
B、证据及时性原则
C、取证流程顺序错误
D、数据加密存储要求
答案：C

9. 某智能家居系统因未实施设备与云端之间的双向身份认证，导致攻击者通过中间人攻击（MITM）拦截并篡改通信数据。在此场景下，以下哪些安全事件最可能发生？（　）
A、攻击者伪造指令远程操控智能门锁，触发异常开锁行为
B、设备因固件版本过低，被攻击者利用漏洞强制刷入恶意固件
C、用户隐私数据（如摄像头监控画面、语音记录）被攻击者实时窃取并出售
D、家庭 Wi-Fi 因设备过多导致网速变慢，影响视频通话流畅度
答案：AC

10. 随着全球进入数字化时代，网络风险呈指数级增长，网络安全威胁趋向智能，网络安全人才缺口大，现有网络安全工具存在局限性。而人工智能可为网络安全带来变革，以下说法正确的是（　　）。
A、人工智能可以检测和预测新兴的未知威胁
B、人工智能使组织能够更快地对网络威胁做出响应
C、人工智能能以高重复性减少人为错误
D、人工智能提高了专业技能要求
答案：ABC

11. 关于网络空间和平利用说法正确的是（　　）。
A、互相尊重
B、零和博弈
C、求同存异
D、包容互信

答案：ACD

12. 汽车产业发展快速，涉及国家经济、交通运输、生产生活等诸多领域，但同时暴露出的汽车数据安全问题和风险隐患也日益突出。国家鼓励汽车数据依法合理有效利用，倡导汽车数据处理者在开展汽车数据处理活动中坚持（　　）。
A、车内处理原则
B、默认不收集原则
C、精度适用范围原则
D、脱敏处理原则
答案：ABCD

13. 某医院拟用人脸识别技术优化挂号流程。根据《人脸识别技术应用安全管理办法》，以下哪些措施是合规的？（　）
A. 同步提供身份证核验作为替代验证方式
B. 将人脸信息与病历数据关联后加密存储于本地服务器
C. 在门诊大厅显著位置公示处理目的和联系方式
D. 因系统升级变更处理方式后，重新进行影响评估
答案：ACD

14. 在信息传播极其迅速的今天，各种数据渗透着我们的生活，蔓延到社会的各行各业，影响我们的学习、工作及社会的发展。以下对于大数据特点的描述，正确的是（　　）。
A、数据体量巨大
B、数据处理速度快
C、数据价值密度高
D、结构化数据为主
答案：AB

15. 地图导航类 App 在现代社会中扮演着非常重要的角色，不仅简化了人们的出行方式，还提供了多种功能和服务来提升用户体验。那么，地图导航类 App 可收集的必要个人信息有（　　）。
A、注册用户移动电话号码
B、位置信息
C、出发地
D、到达地
答案：BCD

16. 车联网是新一代网络通信技术与汽车、电子、道路交通运输等领域深度融合的新兴产业形态。以下关于加强车联网网络安全和数据安全管理工作的措施，叙述正确的是（　　）。
A、各相关企业要建立网络安全和数据安全管理制度，明确负责人和管理机构
B、加强车载信息交互系统、汽车网关、电子控制单元等关键设备和部件安全防护和安全检测
C、鼓励相关企业、机构接入工业和信息化部车联网安全信任根管理平台，协同推动跨车型、跨设施、跨企业互联互认互通
D、 对智能网联汽车、车联网服务平台及联网系统开展网络安全相关监测，及

时发现网络安全事件或异常行为，并按照规定留存相关的网络日志不少于 3 个月
答案：ABC

17. 工业互联网安全是工业生产运行过程中（　　）的统称，涉及工业互联网领域各个环节，其核心任务就是要通过监测预警、应急响应、检测评估、功能测试等手段确保工业互联网健康有序发展。
A、 信息安全
B、制度安全
C、功能安全
D、 物理安全
答案：ACD

18. 等级保护基本要求作为指导开展等级保护的建设整改、等级测评和监督检查等工作的重要标准，其在等级保护技术体系中具有核心地位。以下关于等保 2.0 基本要求的说法，正确的是（　　）。
A、 现标准名为 GB/T 22239-2019《信息安全技术 网络安全等级保护基本要求》
B、在等保 2.0 基本要求附录 A 中，增加安全控制措施控制点的标注及使用说明
C、从一级到四级均在“安全通信网络”、“安全区域边界”和“安全计算环境”中增加了“可信验证”控制点
D、 从三级以上开始增加了“安全管理中心”要求
答案：ABC

19. 物联网是指通过感知设备、按照约定协议，连接（　　），实现对物理和虚拟世界的信息进行处理并作出反应的智能服务系统。
A、 物
B、人
C、系统
D、 信息资源
答案：ABCD

20. 大数据平台涉及物理环境、网络通信、操作系统、数据库、应用系统、数据存储等安全保护，以下安全技术可用于保护大数据平台的是（　　）。
A、 安全分区
B、防火墙
C、系统安全加固
D、 数据防泄漏
答案：ABCD

21. 人工智能，是利用数字计算机或者数字计算机控制的机器模拟、延伸和扩展人的智能，感知环境、获取知识并使用知识获得最佳结果的（　　）。
A、理论
B、方法
C、技术
D、 应用系统
答案：ABCD

22. 结合区块链基础设施运行模式和技术架构，从区块链核心技术功能角度可将区块链基础设施划分为存储层、网络层和扩展层。以下区块链基础设施可能面临的典型安全风险中，属于扩展层安全风险的是（　　）。
A、存储设备安全风险
B、网络流量威胁
C、合约开发漏洞和后门
D、合约运行安全风险
答案：CD

23. 密钥管理对于保证密钥全生命周期的安全性是至关重要的。密钥可以是随机产生、协商产生等不同的方式产生，产生的同时可在密码产品中记录密钥关联信息，其中包括（　　）。
A、密钥长度
B、密钥种类
C、密钥拥有者
D、密钥使用起始、终止时间
答案：ABCD

24. 随着移动应用 App 的应用普及，其安全威胁活动日益频繁，针对移动应用 App 的安全性检测十分必要，常见的移动应用 App 网络安全检测内容有（　　）。
A、身份认证机制检测
B、防钓鱼安全能力检测
C、App 安全漏洞检测
D、通信会话安全机制检测
答案：ABCD

25. 一段时期以来，部分商业网站平台及“自媒体”账号屡屡发生歪曲解读经济政策、造谣传谣等行为，国家网信办决定开展违规采编发布财经类信息专项整治。其中，以下行为描述中，（　　）属于重点打击的违规问题。
A. 胡评妄议、歪曲解读我国财经方针政策、宏观经济数据
B. 散布“小道消息”，以所谓“揭秘”“独家爆料”等为名进行渲染炒作
C. 转载合规稿源财经新闻信息时，恶意篡改、片面曲解等“标题党”行为
D. 充当金融“黑嘴”，恶意唱空或哄抬个股价格，炒作区域楼市波动
答案：ABCD

26. 网络安全事件应急预案应当按照事件发生后的（　　）等因素对网络安全事件进行分级，并规定相应的应急处置措施。
A、危害程度
B、影响范围
C、系统等级
D、关注程度
答案：AB

27. 明文报文传输协议不能有效的防范网络嗅探，具有一定的威胁，以下（　　）属于明文报文传输协议。
A、HTTP 协议

B、Telnet 协议
C、POP 协议
D、SMTP 协议
答案：ABCD

28. 防火墙是一类防范措施的总称，它使内部网络与 Internet 之间或者与其他外部网络互相隔离、限制网络互访来保护内部网络。以下关于防火墙的说法，正确的是（　　）。
A、防火墙的安全策略包括白名单策略、灰名单策略和黑名单策略
B、防火墙不能防止基于数据驱动式的攻击
C、防火墙是外部网络和受保护网络之间的唯一网络通道
D、防火墙支持多种协议的过滤和控制
答案：BCD

29. 在信息安全风险评估已有安全措施识别过程中，安全措施可以分为预防性安全措施和保护性安全措施两种。以下关于安全措施的描述，正确的有（　　）。
A、预防性安全措施可减少安全事件发生后对组织或系统造成的影响
B、保护性安全措施可降低威胁利用脆弱性导致安全事件发生的可能性
C、在识别脆弱性的同时，评估人员应对已采取的安全措施的有效性进行确认
D、安全措施的确认应评估其有效性，即是否真正地降低了系统的脆弱性，抵御了威胁
答案：CD

30. 信息安全系统工程是确保信息系统在其生命周期内具备安全性的一系列过程、方法和技术的集合。它不仅涉及技术层面，还包括管理、政策和人员等多个方面。关于信息安全系统工程，以下描述正确的是（　　）。
A、随着业务需求的变化，信息安全系统也需要不断更新和完善
B、信息安全系统的建设是在 OSI 网络参考模型的各个层面进行的
C、信息安全系统可以脱离业务应用信息系统独立存在
D、识别和评估安全风险是信息安全系统工程的基础工作
答案：ABD

三、判断题 10
1. 书面形式的涉密载体，应在封面或者首页做出国家秘密标志，汇编涉密文件、资料或摘录、引用属于国家秘密内容的应按照其中最低密级和最长保密期限标注。
答案：错

2. 通过伪基站接收附近手机发送的数据，是数据窃密者使用的一种隐蔽的窃密手段。
答案：对

3. 信息安全事件分为有害程序事件等 7 个基本类，蠕虫事件、僵尸网络事件、后门攻击事件均属于有害程序事件的子类。
答案：错

4. 电子取证是证据的获取活动和过程，是信息安全保障反击环节的重要内容，其中拷贝是电子取证的核心过程。
答案：错

5. 网络蠕虫是恶意代码的一种类型，具有自我复制和传播能力，四个功能模块包括探测模块、扫描模块、负载模块、蠕虫引擎模块。
答案：错

6. 可信计算是增强信息系统安全的有效手段，它基于一个硬件安全模块，通过逐级校验建立可信链，进而建立可信计算环境。
答案：对

7. 互联网信息服务，是指通过互联网向上网用户提供信息的服务活动，分为盈利性、非盈利性两类。
答案：错

8. 隔离是将两个环境的边界分开的一种手段。目前实施网络隔离的技术路线主要有三种：网络开关、实时交换和单向连接。
答案：对

9. 一个好的扫描器能对它得到的数据进行分析，帮助我们查找目标主机的漏洞。
答案：对

10. 网络平台不安全，平台所承载的数据就不安全；网络数据不安全，数据所承载的信息就不安全。
答案：对

三、区块链 20

一、单选题 12
1. 公有链与私有链的主要区别是（ ）。
A、公有链使用智能合约，而私有链不使用智能合约
B、公有链更安全，而私有链更高效
C、公有链使用密码学加密算法，而私有链不使用加密算法
D、公有链可以被任何人参与，而私有链仅限于特定的参与者
答案：D

2. 区块链中的零知识证明（Zero-Knowledge Proof）用于解决什么问题（ ）。
A、隐私保护
B、数据完整性验证
C、交易速度优化
D、分布式网络安全
答案：A

3. 区块链是点对点传输、共识机制、加密算法等计算机技术的新型应用模式。

以下关于区块链的描述，不正确的是（　　）。
A、区块链的共识机制可有效防止记账结点信息被篡改
B、区块链可在不可信的网络进行可信的信息交换
C、区块链的身份鉴别不依赖于数字签名技术
D、区块链是一个分布式共享账本和数据库
答案：C

4. 以下关于区块链的去中心化特点，说法不正确的是（　　）。
A、没有中心服务器
B、所有节点权限对等
C、数据分布存储
D、系统低冗余
答案：D

5. 区块链浏览器就是区块链技术的可视化，专门为用户提供（　　）。
A、加入区块链网络的入口
B、区块链技术介绍
C、查询用户身份信息
D、查询区块链上信息
答案：D

6. 下列选项中，（　　）是分布式文件存储系统。
A、HDFS
B、Flume
C、Kafka
D、Zookeeper
答案：A

7. 联盟链更加适用于（　　）。
A、消费互联网
B、产业互联网
C、信息互联网
D、移动互联网
答案：B

8. 某联盟链用于跨境贸易结算，需确保交易隐私和节点通信安全。以下其面临的安全威胁及可能的防御方案对应正确的是（　　）。
A、恶意节点伪造多个身份加入网络，发送虚假交易-使用 TLS 加密 P2P 通信，实施双向证书认证
B、攻击者劫持节点网络连接，使其仅接收篡改后的区块数据-采用零知识证明技术验证交易有效性，隐藏细节
C、交易敏感信息（如金额、参与者）在链上明文存储，被第三方窃取-部署 IP 信誉系统，限制单一实体控制的节点数量
D、攻击者通过恶意智能合约在链上执行计算时，窃取未加密的中间数据-启用同态加密，确保数据在计算过程中保持加密状态
答案：D

9. 某区块链网络要求每笔交易必须经过哈希计算、数字签名和共识验证。用户 A 向用户 B 转账时，攻击者截获交易数据并修改了转账金额，但交易最终被网络拒绝。已知该区块链采用 SHA256 哈希算法和椭圆曲线数字签名（ECDSA）。以下哪一环节直接导致攻击者的篡改行为失效？ （ ）
A、哈希值校验失败，因修改金额后原哈希值不匹配
B、数字签名验证失败，因私钥未泄露，签名无法伪造
C、共识节点发现交易哈希与区块内容不一致
D、网络层加密传输阻止了中间人攻击
答案：B

10. 区块链概念可以理解为是以（ ）为基础，使用共识机制、点对点网络、智能合约等技术结合而成的一种分布式存储数据库技术。
A、量子加密算法
B、非对称加密算法
C、对称密码算法
D、哈希算法
答案：B

11. 区块链技术通过其去中心化、不可篡改性和透明性等特性，为网络安全提供了新的解决方案。以下关于区块链技术特性的描述，正确的是（ ）。
A、透明性使得区块链上的所有用户信息都是公开可见的
B、区块链的去中心化特性使得它比传统系统更慢
C、不可篡改性保证了区块链上的数据绝对安全
D、去中心化使得区块链网络不易受到单点故障的影响
答案：D

12. 区块链系统根据节点准入控制机制与应用场景的不同，可分为（ ）。
A、公有链
B、私有链
C、联盟链
D、混合链
答案：ABC

二、多选题 5
1. 区块链技术因其独特的特性，在网络安全领域有着广泛的应用和潜在的优势，下列选项中，哪些是区块链技术在提升网络安全方面的具体应用或优势？（ ）
A、区块链可以通过增加数据冗余来显著提高数据传输速度
B、智能合约能够自动执行预设规则，减少人为错误和欺诈行为
C、可以通过高级加密技术（如零知识证明）来保护隐私
D、去中心化特性使得区块链网络不易成为 DDoS 攻击的目标
答案：BCD

2. 区块链信息服务提供者对违反法律、行政法规规定和服务协议的区块链信息服务使用者，可以采取以下哪些措施？（ ）
A、依法依约采取警示

B、限制功能使用
C、关闭账号
D、没收账号内的资产
答案：ABC

3. 区块链应用于社会公益慈善领域，可以提高公益慈善的透明度、（ ）、（ ）和失信行为等。
A、可信度
B、避免欺诈
C、可靠性
D、连续性
答案：AB

4. 区块链在数据共享方面的特点有（ ）。
A、不可篡改
B、去中心化
C、透明
D、访问控制权
答案：ABC

5. 区块链中的跨链技术（Cross-chain）解决不了什么问题？（ ）
A、区块链的数据隐私保护
B、区块链节点的身份验证
C、不同区块链之间的数据互通
D、区块链的共识算法优化
答案：ABD

三、判断题 3
1.区块链信息服务提供者不得为不进行真实身份信息认证的用户提供相关服务。
答案：对

2.区块链就是比特币。
答案：错

3.区块链是利用密码技术将共识确认的区块按顺序追加形成的分布式账本。
答案：对

四、人工智能 30

一、单选题 11
1．依据《生成式人工智能服务管理暂行办法》，推动生成式人工智能基础设施和公共训练数据资源平台建设，鼓励采用（ ）的芯片、软件、工具、算力和数据资源。
A、高性能
B、自主研发
C、高能耗效率

D、安全可信
答案：D

2. 某高校实验室研发了一款生成式人工智能模型，仅用于内部学术研究，未向公众开放服务。根据《生成式人工智能服务管理暂行办法》，该实验室的研发活动是否适用本办法？（　）
A、适用，因为涉及生成式人工智能技术
B、适用，但可以豁免部分条款
C、不适用，因其未向境内公众提供服务
D、不适用，但需向主管部门备案
答案：C

3. 某短视频平台上线了一款 AI 生成特效工具，用户可用其生成虚拟场景并导出为视频。根据《人工智能生成合成内容标识办法》，以下哪一做法符合规定？（　）
A、仅在视频末尾添加文字提示“AI 生成”
B、在视频起始画面添加动态水印标识，并在文件元数据中记录平台编码
C、用户导出视频时自动去除所有显式标识以提升观感
D、仅在文件元数据中添加隐式标识，不设置显式标识
答案：B

4. 人工智能（AI）作为一项前沿技术，在提升网络安全防御能力方面展现了巨大潜力。以下哪项不是 AI 在增强网络安全防护中的典型应用场景？（　）
A、恶意软件检测
B、入侵行为分析
C、自动化漏洞扫描
D、电源管理优化
答案：D

5. AI 具有强大的模式识别和数据分析能力，能够帮助安全系统实现智能化、自动化的威胁检测与响应。在以下选项中，哪一项是人工智能在网络安全中用于“自动识别”的典型应用场景？（　）
A、电脑硬件型号
B、异常登录行为
C、软件版本号
D、IP 地址归属地
答案：B

6. 在反垃圾邮件系统中，AI 通过分析邮件内容语义特征（如钓鱼链接模式、恶意附件行为、垃圾关键词变体）实现高精度拦截，其最核心的技术基础是（　）。
A、文本分类
B、特征哈希
C、数据脱敏
D、协议过滤
答案：A

7. （　）是指 AI 通过实时学习正常流量基线（如访问频率、协议合规性、数据

包特征），自动识别偏离模式的恶意行为（如 DDoS 攻击、APT 渗透、数据外传）。
A、流量清洗
B、异常检测
C、流量整形
D、网络隔离
答案：B

8. 在保护人工智能模型的知识产权和防止未经授权的使用方面，不同的技术措施可以起到关键作用。请问以下哪一项技术专门设计用于在 AI 模型中嵌入特定的信息或标识？（ ）
A、模型水印
B、模型加密
C、模型轻量化
D、模型分享
答案：A

9. 生成对抗网络（GAN）因其强大的数据生成能力被用于图像合成等领域，但在网络安全中可能被恶意利用。攻击者通过 GAN 的生成器和判别器对抗训练机制，最可能实现的威胁场景是（ ）。
A、优化防火墙规则
B、生成逼真的钓鱼邮件或恶意代码变种
C、加速数据加密过程
D、提高身份认证速度
答案：B

10. 某医疗机构的 AI 诊断系统被曝存在模型逆向攻击风险，攻击者可通过多次查询 API 重构训练数据。以下哪种技术组合能最优解决该问题？（ ）
A、联邦学习+同态加密
B、差分隐私+ API 调用频率限制
C、模型蒸馏+输入数据模糊化
D、生成对抗网络（GAN）+自动渗透测试
答案：B

11. 随着人工智能技术的快速发展和广泛应用，为企业和个人带来便利的同时，也为网络安全领域带来了新挑战。请将左侧的 AI 技术原理与右侧可能引发的网络安全威胁进行正确匹配：

技术原理	安全威胁
1. 神经网络梯度反向传播	A. 模型窃取攻击（Model Stealing）
2. 自然语言处理（NLP）预训练	B. 深度伪造（Deepfake）音频生成
3. 强化学习的策略可解释性低	C. 自动化钓鱼邮件生成
4. 生成对抗网络（GAN）	D. 黑盒模型决策过程不可控

A、1-A；2-C；3-D；4-B
B、1-B；2-D；3-A；4-C
C、1-C；2-A；3-B；4-D

D、1-D；2-B；3-C；4-A
答案：A

二、多选题 9
1、人工智能技术在网络安全领域的应用非常广泛，能够显著提高网络安全防护的效率和效果。以下关于人工智能在网络安全中的应用描述，正确的是（　　）。
A、利用深度学习技术分析电子邮件以防止垃圾邮件和网络钓鱼
B、采用自然语言处理技术来自动阅读和理解安全报告
C、利用人工智能技术进行用户和实体行为分析，以识别可疑活动
D、人工智能技术可用来增加网络带宽，提高数据传输速率
答案：ABC

2、“AI+安全”范式是指在信息安全领域中应用人工智能技术来增强系统的安全性、检测和预防各种安全威胁。随着其广泛实践应用，网络安全产业将迎来较大变化。以下“AI+安全”范式的应用场景中，描述正确的是（　　）。
A、AI 可以用来识别和过滤钓鱼邮件和其他形式的社会工程攻击
B、使用 AI 算法对发现的所有漏洞进行快速修复
C、通过 AI 监控整个组织的安全状态，实时更新安全策略
D、结合 AI 技术的防火墙可以根据流量模式动态调整规则
答案：ACD

3、某社交媒体平台检测到用户发布的一段音频未声明是否含 AI 生成内容。根据《人工智能生成合成内容标识办法》，平台应采取哪些措施？（　）
A、核验文件元数据中是否存在隐式标识
B、若未核验到隐式标识，直接删除该内容
C、在音频周边添加“疑似生成合成内容”提示标识
D、若检测到显式标识，无需额外操作
答案：AC

4、为防止 AI 训练数据、模型参数或用户隐私等信息在处理、存储和传输过程中被非法获取或泄露，采取有效的安全防护措施至关重要。以下哪几项是防止 AI 数据泄露的可行方法？（　）
A、数据脱敏
B、访问权限控制
C、加密存储
D、增加显示器亮度
答案：ABC

5、在人工智能开发过程中，保护用户隐私需采用系统化的技术手段。以下选项中，哪些技术能直接在隐私保护层面发挥作用，而非仅解决数据安全或模型性能问题？（　）
A、差分隐私
B、联邦学习
C、数据脱敏
D、数据共享
答案：ABC

6. 某金融公司部署了基于深度学习的欺诈交易检测系统，但近期发现有攻击者利用生成对抗样本的方法成功绕过了该系统的检测机制。以下哪些技术或措施能有效提升模型对抗此类攻击的鲁棒性？（ ）
A、在训练集中注入少量对抗样本进行对抗训练
B、使用梯度掩码隐藏模型敏感参数
C、部署输入数据归一化与异常值过滤机制
D、在服务器端部署传统防火墙阻断异常 IP 请求
答案：AC

7. 为了促进生成式人工智能健康发展和规范应用，我国制定了《生成式人工智能服务管理暂行办法》。根据办法内容，以下说法正确的是（ ）。
A、办法自 2023 年 8 月 15 日起施行
B、规定生成式人工智能服务提供者应当依法承担网络信息内容生产者责任，履行网络信息安全义务
C、生成式人工智能服务提供者应当按照《互联网信息服务深度合成管理规定》对图片、视频等生成内容进行标识
D、生成式人工智能服务使用者，是指使用生成式人工智能服务生成内容的个人
答案：ABC

8. 国家坚持发展和安全并重、促进创新和依法治理相结合的原则，采取有效措施鼓励生成式人工智能创新发展，依据《生成式人工智能服务管理暂行办法》，对生成式人工智能服务实行（ ）。
A、开放管理
B、包容审慎
C、分类分级监管
D、分地域限制
答案：BC

三、判断题 10
1、强化学习在网络安全中仅适用于攻击方自动化渗透，防御方无法应用。（ ）
答案：错

2、AI 可以完全替代人类网络安全专家。（ ）
答案：错

3、AI 模型在恶意软件检测中的准确率可达 100%，无需其他辅助手段。（ ）
答案：错

4、区块链技术与 AI 结合可确保训练数据不可篡改，提升模型可信度。（ ）
答案：对

5、零信任架构（Zero Trust）依赖 AI 实现动态访问决策，无需预设信任区域。（ ）
答案：对

6、AI 在日志分析中仅能处理结构化数据，无法解析非结构化文本。（ ）
答案：错

7、深度学习模型可直接用于加密数据的分析而无需解密。（ ）
答案：错

8、在威胁狩猎中，AI 算法的主要作用是主动分析网络行为，发现隐藏的高级持续性威胁（APT）。（ ）
答案：对

9、AI 可通过分析用户登录时间和地理位置模式，实时识别账户劫持行为。（ ）
答案：对

10、对抗样本攻击能欺骗 AI 图像识别系统，但无法影响网络安全检测模型。（ ）
答案：错

五、标准题 230

一、单选题 80
1. GM/Z 4001-2013《密码术语》中，由 IETF 制定的密钥协商协议，定义了通信双方进行身份鉴别、协商加密算法以及生成共享会话密钥的一种方法称为（ ）。
A、lKE 协议
B、IPSec 协议
C、ISAKMP 协议
D、SSL 协议
答案：A

2. GM/Z 4001-2013《密码术语》中，控制密码算法运算的关键信息或参数称为（ ）。
A、密钥
B、密文
C、密码
D、算法
答案：A

3. GM/Z 4001-2013《密码术语》中，加密和解密使用相同密钥的密码算法称为（ ）。
A、公钥密码算法
B、对称密码算法
C、密码杂凑算法
D、非对称密码算法
答案：B

4. GM/T 0034-2014《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（ ）。

A、存在于硬件密码设备之外的所有密钥应加密
B、对密码设备操作应由多个业务管理员实施
C、密钥应有安全可靠的备份恢复机制
D、密钥的生成和使用应在硬件密码设备中完成
答案：B

5. GM/T 0005-2021《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（ ）。
A、Miller-Rabin 算法
B、Berlekamp-Massey 算法
C、最小二乘法
D、中国剩余定理
答案：B

6. 以下关于 GM/T 0034-2014《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（ ）。
A、证书申请和下载可以采用在线或离线两种方式
B、用户签名密钥对和加密密钥对均由用户自己产生
C、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
D、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
答案：B

7. 根据 GB/T 39786-2021《信息安全技术 信息系统密码应用基本要求》中，以下不是设备和计算安全层面的测评对象的是（ ）。
A、数据库管理系统
B、虚拟设备
C、OA 办公系统
D、电子签章系统
答案：C

8. 在 GM/T 0011-2023《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。
A、加密
B、解密
C、杂凑
D、签名
答案：C

9. 根据 GB/T 39786-2021《信息安全技术 信息系统密码应用基本要求》，以下不是设备和计算安全层面第三级信息系统测评指标的是（ ）。
A、身份鉴别
B、远程管理通道安全
C、系统资源访问控制完整性
D、安全接入认证

答案：D

10. 依据 GB/T 20984-2022《信息安全技术 信息安全风险评估方法》要求，应在风险识别基础上开展风险分析，以下关于风险分析的描述，错误的是（　　）。
A、根据威胁频率，以及脆弱性被利用难易程度，计算安全事件发生的可能性
B、根据安全事件造成的影响程度和资产价值，计算安全事件发生后对评估对象造成的损失
C、根据安全事件发生的可能性以及安全事件发生后造成的损失，计算系统资产面临的风险值
D、根据业务所涵盖的系统资产风险值综合计算得出业务风险值
答案：A

11. 在 GM/T 0018-2023《密码设备应用接口规范》中，以下（　　）函数不是对称算法类函数。
A、对称加密
B、对称解密
C、计算 MAC
D、产生随机数
答案：D

12. 根据 GB/T 39786-2021《信息安全技术 信息系统密码应用基本要求》，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（　　）。
A、制定密码应用方案
B、制定密钥安全管理策略
C、投入运行前进行商用密码应用安全性评估
D、定期开展密码应用安全性评估及攻防对抗演习
答案：D

13. 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（　　）。
A、重要数据传输机密性
B、身份鉴别
C、日志记录完整性
D、不可否认性
答案：B

14. 依据 GB/T 20984-2022《信息安全技术 信息安全风险评估方法》，在对威胁进行分类前，应识别威胁的来源，威胁来源包括环境、意外和人为三类。以下描述中，可被划分为意外来源的是（　　）。
A、 电磁干扰
B、 非人为因素导致的软件故障
C、 人为因素导致的资产保密性遭到破坏
D、 鼠蚁虫害
答案：B

15. 根据 GM/T 0116-2023《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（　　）。
A、可重复性和可再现性原则
B、经济性原则
C、客观公正性原则
D、结果完善性原则
答案：B

16. 根据 GM/T 0029-2014《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。
A、系统配置
B、证书导入
C、密钥导入
D、日志记录
答案：A

17. GM/T 0033-2023《时间戳接口规范》适用范围是（　　）。
A、基于对称加密算法的产品和应用
B、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
C、基于哈希算法的产品和应用
D、所有密码学相关产品和应用
答案：B

18. 在 GM/T 0123-2022《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（　　）
A、SM2-1 数字签名算法 1.2.156.10197.1.301.1
B、公钥密码算法 1.2.156.10197.1.300
C、基于 SM2 算法和 SM3 算法的签名 1.2.156.10197.1.501
D、《SM2 椭圆曲线公钥密码算法》1.2.156.10197.6.1.1.3
答案：A

19. 在 GM/T 0123-2022《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
A、生物特征识别
B、登录口令
C、基于数字证书的数字签名
D、验证码
答案：C

20. GM/T 0036-2014《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（　　）。
A、安全模块只需支持 SM1/SM4 算法
B、门禁卡需要实现一卡一密
C、门禁卡与非接触读卡器间需要进行身份鉴别
D、门禁卡与非接触读卡器间需要进行数据加密通讯
答案：A

21. GM/T 0036-2014《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（　　）。
A、一卡一密
B、一次一密
C、一次三密
D、一次多密
答案：A

22. GM/T 0036-2014《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（　　）。
A、GM/T 0032
B、GM/T 0033
C、GM/T 0034
D、GM/T 0035
答案：D

23. GM/T 0031-2014《安全电子签章密码技术规范》中的规定范围是（　　）。
A、电子印章和电子签章的数据结构、密码处理流程
B、电子印章数据结构
C、电子签章数据结构
D、电子签章密码处理流程
答案：A

24. GM/T 0031-2014《安全电子签章密码技术规范》中对制章人的描述正确的是（　　）。
A、制章人只能是单位证书
B、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
C、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
D、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
答案：C

25. 根据 GB/T 39786-2021《信息安全技术 信息系统密码应用基本要求》，以下可用于应用和数据安全层面身份鉴别保护的密码产品是（）。
A、IPSec VPN 设备
B、智能密码钥匙
C、电子文件密码应用系统
D、电子门禁系统
答案：B

26. GB/T 39786-2021《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。
A、应
B、宜
C、可
D、须

答案：A

27. 在依据 GBT 43206-2023《信息安全技术 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。
A、采用 SM3-HMAC 算法计算消息鉴别码
B、仅采用 SM3 算法计算杂凑值
C、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
D、使用 SM3 和 SM2 算法计算签名值
答案：B

28. 在 GM/T 0034-2014《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（ ）。
A、改变系统的配置如无上级主管批准，操作时应有双人在场
B、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
C、对 CA 系统的每次操作都应记录
D、未经批准不得在服务器上安装任何软件
答案：A

29. 在 GM/T 0034-2014《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（ ）。
A、进入管理区的人员只需使用身份识别卡
B、所有的墙体应采用高强度防护墙
C、管理区所有的房间不应安装窗户
D、人员进出管理区要有日志记录
答案：A

30. 依据 GM/T 0037-2014《证书认证系统检测规范》，对于证书认证系统的审计功能的检测，下列选项描述不正确的是（ ）。
A、审计数据只能被审计员修改
B、审计过的记录应有明显标记
C、审计应能验证记录的签名
D、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
答案：A

31. 依据 GM/T 0037-2014《证书认证系统检测规范》，以下描述不正确的是（ ）。
A、RA 应能提供证书下载
B、日志应能按操作者进行查询
C、审计数据仅能由审计员更改
D、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
答案：C

32. 依据 GM/T 0037-2014《证书认证系统检测规范》，证书认证系统采用的证书格式应符合（ ）的要求。

A、GM/T 0015《基于 SM2 密码算法的数字证书格式规范》
B、GM/T 0092《基于 SM2 算法的证书申请语法规范》
C、GM/T 0014《数字证书认证系统密码协议规范》
D、GM/T 0043《数字证书互操作检测规范》
答案：A

33. 在 SM2 密钥交换协议中，依据 GM/T 0003.3-2012《SM2 椭圆曲线公钥密码算法 第 3 部分：密钥交换协议》，用户 A 和 B 最终协商出的共享密钥 K 的长度由哪个参数决定？
A、随机数 r_A 的长度
B、椭圆曲线基点 G 的阶 n
C、密钥派生函数 KDF 的输出长度 klen
D、用户标识 ID_A 和 ID_B 的长度
答案：C

34. 依据 GM/T 0003.3-2012《SM2 椭圆曲线公钥密码算法 第 3 部分：密钥交换协议》，在密钥交换协议中，若响应方 B 计算出的椭圆曲线点 V 为无穷远点，应如何处理？（ ）
A、重新生成随机数 r_B
B、终止协商并报错
C、使用备用曲线参数
D、忽略该点继续计算
答案：B

35. 依据 GM/T 0037-2014《证书认证系统检测规范》，关于 RA 对申请信息的审核，以下各项描述中不正确的是（ ）。
A、应能提供对申请信息审核的界面
B、应能将审核不通过的信息返回到录入界面
C、应能自动使操作员对其操作行为进行签名
D、应能自动批量对申请信息进行审核
答案：D

36. 依据 GB/T 43207-2023《信息安全技术 信息系统密码应用设计指南》，下列关于密码支撑平台方案的设计内容描述错误的是（ ）。
A、密码服务机构的确定、接入方式和服务策略
B、提供的密码支撑方式（如租密码机方式、租密码服务器方式）
C、接口和功能遵循的标准
D、根据审计策略，为日志记录设计密码保护机制
答案：D

37. 依据 GB/T 43207-2023《信息安全技术 信息系统密码应用设计指南》，下列关于业务应用的密码应用方案设计内容描述错误的是（ ）。
A、为角色分配密钥,明确密钥载体,设计系统的密钥管理策略
B、梳理业务数据,根据数据安全需求,为重要数据设计密码保护机制
C、接口和功能遵循的标准
D、根据审计策略,为日志记录设计密码保护机制

答案：C

38. 某金融机构的核心交易系统因遭受分布式拒绝服务（DDoS）攻击，导致系统长时间中断，大量用户无法进行交易，恢复系统需耗费巨额资金。根据 GB/T 20986-2023《信息安全技术 网络安全事件分类分级指南》，该事件最可能被判定为哪一级别的网络安全事件？（ ）
A、一般事件（四级）
B、较大事件（三级）
C、重大事件（二级）
D、特别重大事件（一级）
答案：C

39. 某政府网站首页被篡改为含有违法内容的页面，虽未造成数据泄露，但引发社会广泛关注。根据 GB/T 20986-2023《信息安全技术 网络安全事件分类分级指南》，该事件应归类为（ ）。
A. 网络攻击事件
B. 信息内容安全事件
C. 数据安全事件
D. 违规操作事件
答案：A

40. 依据 GM/T 0009-2023《SM2 密码算法使用规范》，SM2 椭圆曲线公钥密码算法的辅助函数不包括（ ）。
A、密码杂凑函数
B、密钥派生函数
C、随机数发生器
D、填充函数
答案：D

41. 依据 GM/T 0009-2023《SM2 密码算法使用规范》，使用 SM2 密码算法对数据进行加密的过程中调用了（ ）密码算法。
A、SM1
B、SM3
C、SM4
D、ZUC
答案：B

42. 依据 GM/T 0009-2023《SM2 密码算法使用规范》，若 n 为 SM2 椭圆曲线的阶，下列选项中（ ）属于合规的私钥取值。
A、n
B、2n
C、n-1
D、n-2
答案：D

43. 依据 GM/T 0133-2024《关键信息基础设施密码应用要求》，下列关于密钥管

理要求描述不正确的是（　）。
A、应保证密钥数据生命周期的安全性，确保公钥及其他密钥不被非授权访问、使用、泄露、修改和替换
B、应根据密钥管理策略进行密钥使用，保证不同业务应用、不同类型和级别的数据使用不同的密钥
C、应根据密钥管理策略执行密钥更新
D、应根据密钥管理策略执行密钥备份,保证密钥的可用性
答案：A

44. GM/T 0133-2024《关键信息基础设施密码应用要求》中明确了攻防对抗演习具体内容，包括但不限于分析识别密码应用脆弱性，开展验证或模拟攻击和防御，下列选项中不属于密码应用脆弱性问题的是（　）。
A、密码功能被旁路问题
B、密码设备冗余部署问题
C、密码产品和服务错误配置问题；
D、用户非法操作导致的问题
答案：B

45. 依据 GM/T 0133-2024《关键信息基础设施密码应用要求》，关键信息基础设施边界内各等级保护对象，应按照自身的安全保护等级符合（　）的要求。
A、GB/T 39786-2020
B、GB/T 39786-2021
C、GB/T 39686-2020
D、GB/T 39686-2021
答案：B

46. GM/T 0014-2023《数字证书认证系统密码协议规范》描述了 CA、KMC、LDAP 等公钥基础设施（PKI）之间的连接。PKI 主要用于解决什么问题（　）。
A、私钥的机密保护
B、公钥属于谁
C、非对称密码算法的实现
D、公钥的机密性保护
答案：B

47. 某电商平台在处理用户订单信息时，使用 SM3 算法生成摘要。依据 GM/T 0004-2012《SM3 密码杂凑算法》，SM3 算法生成的消息摘要长度是多少？（ ）
A、128 位
B、256 位
C、512 位
D、1024 位
答案：B

48. 某互联网公司需要向电子认证服务使用密码许可单位采购数字证书，用于部署站点证书。根据 GM/T 0014-2023《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（　）。
A、向 KM 申请加密密钥对

B、签发签名证书
C、签发加密证书
D、自己生成加密密钥对
答案：D

49. 根据 GM/T 0028-2024《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。
A、1
B、2
C、3
D、4
答案：C

50. 管理员为新采购的一批未激活令牌进行启用操作，过程中验证了令牌生成的动态口令，操作完成后令牌状态变为 “就绪”。依据 GM/T 0021-2023《动态口令密码应用技术规范》，该操作属于（ ）。
A、锁定
B、激活
C、挂起
D、废止
答案：B

51. 依据 GM/T 0001.3-2012《祖冲之序列密码算法 第 3 部分：基于祖冲之算法的完整性算法》，在 128-EIA3 完整性算法中，消息认证码（MAC）的长度被定义为 32 比特。若某条信令消息的长度为 1000 比特，为计算其 MAC 值，ZUC 算法需要产生的密钥字总数 L 是多少？（ ）
A、32
B、33
C、34
D、35
答案：C

52. 根据 GM/T 0003.2-2012《SM2 椭圆曲线公钥密码算法 第 2 部分：数字签名算法》，在 SM2 签名生成过程中，若计算出的 r=0 或 r+k=n，应如何处理？（ ）
A、直接输出签名
B、重新生成随机数 k
C、更换私钥
D、更换公钥
答案：B

53. 依据 GM/T 0001.1-2012《祖冲之序列密码算法 第 1 部分：算法描述》，在 ZUC 算法的初始化阶段，非线性函数 F 的输出 W 经过怎样的处理后才输入 LFSR？（ ）
A、直接输入
B、右移 1 位

C、左移 1 位
D、与常量异或
答案：B

54. 依据 GM/T 0001.1-2012《祖冲之序列密码算法 第 1 部分：算法描述》，ZUC 算法中，线性反馈移位寄存器（LFSR）的每个寄存器单元的长度是多少比特？（ ）
A、16 比特
B、31 比特
C、32 比特
D、128 比特
答案：B

55. 依据 GM/T 0001.2-2012《祖冲之序列密码算法 第 2 部分：基于祖冲之算法的机密性算法》，机密性算法需要生成一定长度的密钥流来对明文进行加解密。若需要加密一段长度为 253 比特的明文消息流（IBS），则至少需要生成多少个 32 比特的密钥字？（ ）
A、7 个
B、8 个
C、9 个
D、10 个
答案：B

56. 依据 GM/T 0001.2-2012《祖冲之序列密码算法 第 2 部分：基于祖冲之算法的机密性算法》，以下哪项不是机密性算法的输入参数？（ ）
A、COUNT
B、BEARER
C、MAC
D、CK
答案：C

57. 依据 GM/T 0001.2-2012《祖冲之序列密码算法 第 2 部分：基于祖冲之算法的机密性算法》，机密性算法的输出 OBS 是如何得到的？（ ）
A、OBS = IBS ⊕ KEY
B、OBS = IBS ⊕ IV
C、OBS = IBS ⊕ 密钥流 k
D、OBS = IBS ⊕ COUNT
答案：C

58. 依据 GM/T 0001.3-2012《祖冲之序列密码算法 第 3 部分：基于祖冲之算法的完整性算法》，以下哪项不是完整性算法的输入参数？（ ）
A、IK
B、M
C、TAG
D、DIRECTION
答案：C

59. 依据 GM/T 0001.4-2024《祖冲之序列密码算法 第 4 部分鉴别式加密机制》，GHASH 函数中使用的有限域是？（ ）
A、GF(2^64)
B、GF(2^128)
C、GF(2^256)
D、GF(2^512)
答案：B

60. 依据 GM/T 0001.4-2024《祖冲之序列密码算法 第 4 部分鉴别式加密机制》，ZUC-GXM 机制中，要求初始向量 IV 具备什么特性？（ ）
A、可重复使用
B、必须为全 0
C、不应重复使用
D、必须为随机数
答案：C

61. 我国商用密码标准中的密码杂凑算法是 SM3 算法，目前已被广泛被使用于各个领域。依据 GM/T 0004-2012《SM3 密码杂凑算法》，SM3 的压缩函数每次处理的消息分组长度是多少？（ ）
A、512 比特
B、256 比特
C、1024 比特
D、128 比特
答案：A

62. SM4 算法的轮函数 F 的结构中，根据 GM/T 0002-2012《SM4 分组密码算法》，哪一步是合成置换 T 的作用？（ ）
A、异或轮密钥
B、循环左移
C、S 盒替换
D、线性变换 L
正确答案：D

63. 在 SM2 算法中，若使用压缩表示形式表示椭圆曲线上的点，依据 GM/T 0003.1-2012《SM2 椭圆曲线公钥密码算法 第 1 部分：总则》，PC 字节的可能取值是什么？（ ）
A、00 或 01
B、02 或 03
C、04 或 05
D、06 或 07
答案：B

64. 依据 GM/T 0003.4-2012《SM2 椭圆曲线公钥密码算法 第 4 部分：公钥加密算法》，密文 C 的格式为以下哪三种数据的拼接？（ ）
A、C1 || C2 || C3

B、C1 || C3 || C2
C、C2 || C1 || C3
D、C3 || C1 || C2
答案：B

65. 依据 GM/T 0003.5-2012《SM2 椭圆曲线公钥密码算法 第 5 部分：参数定义》SM2 推荐使用的椭圆曲线是定义在什么域上的？（ ）
A、二进制域
B、素数域
C、扩展域
D、复合域
答案：B

66. 某科技公司计划对其生产的密码产品依据 GM/T 0028-2024《密码模块安全技术要求》进行评级。其中，（ ）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。
A、1
B、2
C、2 和 3
D、3 和 4
答案：D

67. 以下哪个部件不能作为 GM/T 0028-2024《密码模块安全技术要求》中规定的密码模块控制输入接口？（ ）
A、LED 指示灯
B、触摸屏
C、芯片管脚
D、网口
答案：A

68. 依据 GM/T 0039-2024《密码模块安全检测要求》，密码模块在哪种状态下应禁止通过“数据输出接口”输出数据？（ ）
A、正常运行状态
B、自测试通过后
C、执行手动输入或处于错误状态时
D、密码主管角色登录时
答案：C

69. 根据 GM/T 0039-2024《密码模块安全检测要求》，密码模块的可信信道必须具备哪种特性？（ ）
A、允许通过公共网络传输明文密钥分量
B、所使用的物理端口应与其他物理端口实现物理隔离
C、传输速度必须高于其他数据接口
D、只能用于传输加密后的敏感安全参数
答案：B

70. 根据 GM/T 0039-2024《密码模块安全检测要求》，密码模块的运行前自测试必须在何时完成？（ ）
A、在操作员发出自测试命令后
B、在密码模块提供任何数据输出之前
C、在密码模块进入错误状态后
D、在每日定时维护时段内
答案：B

71. 如果密码模块允许操作员变换角色，且新角色之前未被鉴别，根据 GM/T 0039-2024《密码模块安全检测要求》，模块应如何处理？（ ）
A、允许短暂访问，并记录日志
B、拒绝该操作，维持原角色权限
C、鉴别该操作员能否担任新角色
D、自动降级到最低权限角色
答案：C

72. 关于密码模块中敏感安全参数的置零，依据 GM/T 0039-2024《密码模块安全检测要求》，下列哪项描述是正确的？（ ）
A. 可以使用另一个未受保护的敏感安全参数进行覆盖
B. 置零操作可以被高级用户中断
C. 置零应确保参数无法被恢复和重用
D. 仅需对明文形式的敏感安全参数进行置零
答案：C

73. 依据 GM/T 0134-2024《密码模块安全设计指南》，密码模块的密码边界划定中，以下哪类模块的密码边界不包括操作系统？（ ）
A、硬件密码模块
B、软件密码模块
C、固件密码模块
D、混合密码模块
答案：B

74. 依据 GM/T 0134-2024《密码模块安全设计指南》，（ ）必须使用可信信道传输敏感信息。
A、安全一级模块
B、安全二级模块
C、安全三级及以上模块
D、所有模块均需使用
答案：C

75. 依据 GM/T 0134-2024《密码模块安全设计指南》，密码模块的运行前自测试不包括以下哪项内容？（ ）
A、软件/固件完整性测试
B、旁路测试
C、密码算法性能测试
D、关键功能测试

答案：C

76. 依据 GM/T 0134-2024《密码模块安全设计指南》，密码模块的鉴别机制强度要求中，单次尝试成功的概率不得高于（ ）。
A、1/1000
B、1/10,000
C、1/100,000
D、1/1,000,000
答案：D

77. 在 GM/T 0139-2024《信息系统密码应用安全管理体系》中，密码应用安全管理体系遵循的管理循环是（ ）。
A、SDLC
B、PDCA
C、DevOps
D、Agile
答案：B

78. 依据 GM/T 0139-2024《信息系统密码应用安全管理体系》，密码应用安全风险评估中，以下哪项不属于风险评估的步骤？（ ）
A、识别资产
B、识别威胁
C、制定应急计划
D、分析风险
答案：C

79. GM/T 0139-2024《信息系统密码应用安全管理体系》规定，密钥管理员与以下哪个岗位不能兼任？（ ）
A、密码操作员
B、系统管理员
C、密码安全审计员
D、网络管理员
答案：C

80. 在 GM/T 0037-2014《证书认证系统检测规范》中，以下各项仅用于产品检测的是（ ）。
A、系统初始化
B、岗位及权限管理
C、多层结构支持
D、网络结构
答案：A

二、多选题 130
1. 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（ ）。
A、算法标识

B、密钥标识
C、设备标识
D、协议标识
答案：AD

2. 某部门在部署基于 SM2 密码算法的证书认证系统时，依据 GM/T 0034-2014《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》，关于系统中的安全管理，以下说法正确的有（ ）
A、要设置不同级别的管理员，明确各自权限
B、对管理员的操作要进行审计记录
C、无需对系统进行安全漏洞检测
D、定期对系统的安全策略进行评估和更新
答案：ABD

3. 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。
A、密钥生成
B、密钥分发
C、密钥导入
D、密钥销毁
答案：ABCD

4. GM/T 0010-2023《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（ ）。
A、加密和签名消息语法
B、加密和签名操作结果的标准化封装
C、对象标识符
D、椭圆曲线参数语法
答案：ABCD

5. 在 GM/T 0019-2023《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（ ）。
A、计算会话密钥
B、单块加密运算
C、结束解密运算
D、多组数据消息鉴别码运算
答案：AB

6. 依据 GB/T 20984-2022《信息安全技术 信息安全风险评估方法》中关于风险评估基本要素之间的关系，描述正确的是（ ）。
A、风险要素的核心是资产，而资产存在脆弱性
B、安全措施的实施通过降低资产脆弱性被利用难易程度，抵御外部威胁
C、脆弱性通过利用资产存在的威胁导致风险
D、风险转化成安全事件后，会对资产的运行状态产生影响
答案：ABD

7. 参照 GM/T 0024-2023《SSL VPN 技术规范》实现的 SSL 协议，以下说法正确的是（ ）。
A、Hello 消息中，双方交换的随机数用于派生出主密钥
B、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
C、IBC_SM4_SM3 密码套件中采用 SM9 算法实现身份鉴别
D、生成密钥的 PRF 算法可用 SM3 实现
答案：ABCD

8. 根据 GM/T 0005-2021《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（ ）。
A、通过样本数量是 970
B、通过样本数量是 975
C、通过样本数量是 981
D、通过样本数量是 985
答案：CD

9. 在 GM/T 0027-2014《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（ ）。
A、软件要求
B、性能要求
C、环境适应性要求
D、可靠性要求
答案：ABCD

10. 根据 GM/T 0027-2014《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（ ）。
A、接口
B、芯片
C、线路传输
D、密钥安全
答案：ABC

11. 根据 GM/T 0027-2014《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（ ）。
A、密码算法
B、密钥管理
C、多应用安全
D、线路传输安全
答案：ABCD

12. 在 GM/T 0016-2023《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（ ）。
A、管理员 PIN
B、用户 PIN
C、设备验证密钥

D、报文鉴别码 MAC
答案：AB

13. 在 GM/T 0016-2023《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（　）
A、一个设备中可以存在多个应用
B、不同的应用之间可以共享数据
C、应用由管理员 PIN、用户 PIN、文件和容器组成
D、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
答案：ACD

14. 在 GM/T 0017-2023《智能密码钥匙密码应用接口数据格式规范》中，命令报文和响应报文可能出现的情况有（　）。
A、命令报文无数据，响应报文无数据
B、命令报文无数据，响应报文有数据
C、命令报文有数据，响应报文无数据
D、命令报文有数据，响应报文有数据
答案：ABCD

15. 在 GM/T 0048-2016《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（　）。
A、文件读写性能
B、对称算法性能
C、非对称算法性能
D、杂凑算法性能
答案：ABCD

16. 在 GM/T 0048-2016《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（　）。
A、ECB 模式
B、CBC 模式
C、CFB 模式
D、CTR 模式
答案：AB

17. 根据 GM/T 0048-2016《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（　）
A、文件读写性能
B、应用初始化性能
C、非对称算法性能
D、杂凑算法性能
答案：ACD

18. 在 GM/T 0063-2018《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）
A、设备-->应用-->容器-->证书
B、设备-->应用-->文件
C、设备-->容器-->应用-->证书-->文件
D、设备-->容器-->应用-->证书
答案：AB

19. 在 GM/T 0063-2018《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（ ）。
A、ECC 生成密钥协商参数并输出
B、ECC 产生密钥协商数据并导出会话密钥
C、ECC 计算会话密钥
D、ECC 签名
答案：ABC

20. 根据 GM/T 0018-2023《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（ ）。
A、密码机
B、密码卡
C、智能密码终端
D、扫描仪
答案：ABC

21. 在 GM/T 0018-2023《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（ ）。
A、杂凑运算初始化
B、多包杂凑运算
C、杂凑运算结束
D、杂凑运算结果校验
答案：ABC

22. 在 GM/T 0018-2023《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（ ）。
A、模长
B、模 N
C、公钥指数
D、素数 p 和 q
答案：ABC

23. 根据 GM/T 0018-2023《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（ ）。
A、密钥管理
B、数据加密
C、应用管理
D、随机数生成
答案：ABD

24. 在 GM/T 0121-2022《密码卡检测规范》中，密码卡检测项目可包括（　）。
A、功能检测
B、性能检测
C、安全性检测
D、虚拟化检测
答案：ABCD

25. 在 GM/T 0121-2022《密码卡检测规范》中，在就绪状态下，密码卡不能执行（　）操作。
A、满足权限时，能够提供用户密钥管理和密码运算等功能
B、通过删除操作员操作使密码卡进入初始状态
C、生成设备密钥对和保护密钥的生成操作
D、恢复设备密钥对和保护密钥的操作
答案：BCD

26. 在 GM/T 0121-2022《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（　）。
A、在指定的操作系统中应能够正确地安装和卸载
B、宜支持多个密码卡设备同时使用和操作的基本要求
C、宜与密码卡具备安全绑定机制
D、不可支持多个密码卡设备同时使用和操作
答案：ABC

27. 在 GM/T 0022-2023《IPSec VPN 技术规范》中，IPSec VPN 需要使用（　）类型的密钥。
A、设备密钥
B、工作密钥
C、会话密钥
D、存储密钥
答案：ABC

28. 根据 GM/T 0023-2023《IPSec VPN 网关产品规范》，以下对于 IPSec VPN 中的密钥说法错误的是（　）。
A、设备密钥可以明文导出
B、工作密钥应存储于非易失性存储区
C、设备证书可以明文发送
D、设备密钥应在断电时销毁
答案：ABD

29. 根据 GM/T 0023-2023《IPSec VPN 网关产品规范》，以下哪些属于 IPSec VPN 产品性能参数（　）。
A、加解密吞吐
B、加解密时延
C、每秒新建隧道数
D、最大并发隧道数

答案：ABCD

30. 根据 GM/T 0024-2023《SSL VPN 技术规范》， SSL VPN 中非对称密码算法用于（ ）。
A、身份鉴别
B、数字签名
C、密钥交换
D、数据报文加密
答案：ABC

31. 根据 GM/T 0024-2023《SSL VPN 技术规范》，下列哪些是标准规定的密码套件（ ）。
A、ECC_SM4_SM3
B、IBC_SM4_SM3
C、ECDHE_SM4_SM3
D、RSA_SM4_SM3
答案：ABCD

32. 在 GM/T 0024-2023《SSL VPN 技术规范》中，工作密钥包括（ ）。
A、签名密钥对
B、加密密钥对
C、数据加密密钥
D、校验密钥
答案：CD

33. 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（ ）。
A、超级管理员
B、系统管理员
C、安全管理员
D、系统审计员
答案：BCD

34. 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（ ）。
A、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
B、用户访问行为，包括用户、时间、访问资源、结果
C、异常事件，包括认证失败、非法访问异常事件的记录
D、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
答案：ABC

35. 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。
A、硬盘
B、内存
C、易失性存储介质

D、非易失性存储介质
答案：AD

36. 在 GM/T 0026-2023《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（　）。
A、安全策略的配置
B、密钥的生成
C、管理员的产生
D、设备零部件的组装
答案：ABC

37. 在 GM/T 0049-2016《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（　）。
A、检测密码键盘是否存在通风孔或缝，若不存在则继续检测
B、通过安全 2 级的检测
C、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
D、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
答案：ABCD

38. 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（　）。
A、基本测试项目全部通过
B、基本测试项目没有通过（某些可选测试项可以不测）
C、安全要求检测项目全部通过 4 级检测。
D、安全要求中的非关键要求可不通过 4 级检测
答案：AC

39. 根据 GM/T 0045-2016《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（　）。
A、主密钥
B、次主密钥
C、数据密钥
D、设备密钥
答案：ABC

40. 根据 GM/T 0045-2016《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（　）。
A、磁条卡应用
B、IC 卡应用
C、基础密码运算服务
D、设备管理服务
答案：ABC

41. 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（　）。

A、未初始化状态指示
B、管理员生成
C、服务端口配置
D、管理端口配置
答案：ABCD

42. 根据 GM/T 0030-2014《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（　）。
A、参数查询
B、密钥备份
C、状态查询
D、密钥恢复
答案：AC

43. 根据 GM/T 0030-2014《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（　）。
A、管理密钥的使用可以对应用系统开放
B、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
C、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
D、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
答案：BCD

44. 根据 GM/T 0059-2018《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（　）。
A、管理员操作行为，包括登录认证、系统配置、密钥管理等操作
B、异常事件，包括认证失败、非法访问等异常事件的记录
C、如与设备管理中心连接，则对相应操作进行记录
D、对应用接口中密钥管理相关调用记录日志
答案：ABCD

45. 依据 GB/T 31168-2023《信息安全技术 云计算服务安全能力要求》，根据资源使用情况对提供给云服务客户的云服务功能进行分类，主要分为（　）。
A、应用能力类型
B、基础设施能力类型
C、平台能力类型
D、业务能力类型
答案：ABC

46. 根据 GM/T 0059-2018《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（　）。
A、设备管理类函数
B、对称算法运算类函数
C、用户文件操作类函数
D、杂凑运算类函数
答案：ABCD

47. 根据 GM/T 0029-2014《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。
A、密码运算功能
B、随机数发生器
C、存储的敏感信息
D、管理功能
答案：ABC

48. 根据 GM/T 0029-2014《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。
A、智能密码钥匙
B、智能 IC 卡
C、口令
D、证书链
答案：AB

49. 在 GM/T 0033-2023《时间戳接口规范》中，提及的时间戳响应消息体部分有（　）。
A、时间戳信息摘要值
B、时间戳证书序列号
C、时间戳签名值
D、时间戳签名算法标识符
答案：ABCD

50. 在 GM/T 0123-2022《时间戳服务器密码检测规范》中，设备自检包括（　）。
A、上电自检
B、周期自检
C、复位自检
D、接收指令后自检
答案：ABCD

51. 在 GM/T 0123-2022《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。
A、电子邮件
B、文件
C、HTTP
D、SOAP
答案：ABCD

52. GM/T 0036-2014《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。
A、门禁卡
B、门禁读卡器
C、前台管理系统

D、后台管理系统
答案：ABD

53. 根据 GM/T 0036-2014《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（　）。
A、密钥管理子系统
B、密钥管理母系统
C、发卡子系统
D、发卡母系统
答案：AC

54. 在 GM/T 0036-2014《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（　）。
A、生成密钥
B、注入密钥
C、刷卡开门
D、密钥分散
答案：ABD

55. GM/T 0036-2014《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（　）。
A、SM4
B、SM1
C、DES
D、SM7
答案：ABD

56. 某公司采购了一批动态口令令牌，用于其 OA 系统对登录用户的身份鉴别。这批动态口令令牌处于出厂状态，依据 GM/T 0021-2023《动态口令密码应用技术规范》，以下说法正确的是（　）。
A、此时令牌处于未激活状态，此时不对该令牌的口令进行鉴别
B、令牌激活后令牌处于就绪状态，此时令牌用于口令鉴别
C、连续输入多次 PIN 码错误后，令牌进入作废状态，此时不对该令牌的口令进行鉴别
D、令牌被挂起后处于挂起状态，此时不对该令牌的口令进行鉴别
答案：ABD

57. 某省厅 OA 系统通过基于动态口令对用户进行身份鉴别，对于动态口令系统来说种子密钥管理系统的安全防护至关重要。以下属于 GM/T 0021-2023《动态口令密码应用技术规范》中种子密钥管理系统的种子密钥存储的合规方式有（　）。
A、储在密码设备内
B、加密后存储在密码设备以外的位置(例如数据库),且加密所使用的密钥加密密钥存储在密码设备内
C、明文存储与数据库中
D、通过哈希算法处理后存储于数据库中

答案：AB

58. GM/T 0031-2014《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。
A、证书有效期过期错误
B、密钥用法不正确
C、证书信任链验证失败
D、证书状态已吊销
答案：BC

59. 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（　）。
A、机密性
B、完整性
C、来源的真实性
D、不可否认性
答案：BCD

60. 在 GM/T 0071-2019《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（　）。
A、获取签名算法、杂凑算法标识
B、调用杂凑算法服务对文件内容明文计算摘要
C、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
D、将签名值、算法标识和签名证书按顺序填充至安全属性中
答案：ABCD

61. 在 GM/T 0011-2023《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。
A、产生 SM2 密钥对
B、执行 SM2 加/解密
C、执行 SM2 签名运算
D、杂凑运算
答案：ABC

62. 在 GM/T 0011-2023《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（　）。
A、平台启动后，外部实体向平台发送完整性度量报告的请求
B、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
C、平台将 PCR 的值， PIK 对 PCR 值的签名和 PIK 证书发送给验证者
D、可信密码模块将 PCR 的值进行加密
答案：ABC

63. GM/T 0037-2014《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（　）。
A、应能提供录入和修改证书申请信息的界面

B、应能选择所申请数字证书的密钥类型及长度
C、应支持批量证书申请信息的导入
D、应能自动使操作员对其操作行为进行签名
答案：ABD

64. GM/T 0037-2014《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（ ）。
A、签发系统服务器
B、注册系统服务器
C、LDAP 服务器
D、OCSP 服务器
答案：ABCD

65. 以下密码设备可被 GM/T 0051-2016《密码设备管理 对称密钥管理技术规范》管理的是（ ）。
A、密码机
B、密码卡
C、智能 IC 卡
D、智能密码钥匙
答案：AB

66. 在 GM/T 0051-2016《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（ ）。
A、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
B、与设备管理结合，根据密钥状态支持密钥申请主动上报
C、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
D、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
答案：ABCD

67. 在 GM/T 0051-2016《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（ ）。
A、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
B、对用户主动操作的管理事件进行审计
C、记录服务器状态
D、对服务器状态进行审计
答案：ABC

68. GM/T 0008-2012《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（ ）。
A、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
B、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

C、防护措施的有效性必须通过检测
D、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。
答案：ABC

69. 根据 GM/T 0035.2-2014《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。
A、机密性
B、完整性
C、防冲突
D、抗抵赖
答案：ABD

70. GM/T 0107-2021《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（ ）。
A、管理类密钥
B、交易类密钥
C、发卡机构公钥
D、发卡机构私钥
答案：AB

71. GM/T 0107-2021《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（ ）。
A、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
B、已归档的密钥不应返回到操作使用中
C、已归档密钥不能影响在用的密钥的安全
D、已归档的密钥可以重新恢复并加以使用
答案：ABC

72. 根据 GM/T 0104-2021《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（ ）。
A、虚拟密码机的镜像文件应进行签名保护
B、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
C、虚拟密码机的镜像文件无需进行签名保护
D、云服务器密码机不需要对虚拟密码机镜像进行验证
答案：AB

73. GM/T 0104-2021《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（ ）。
A、SM1
B、SM2
C、SM3
D、SM4
答案：BCD

74. GM/T 0104-2021《云服务器密码机技术规范》规定设备的管理检测包括（　）。
A、管理操作检测
B、管理登录检测
C、管理接口检测
D、日志审计检测
答案：ABCD

75. GM/T 0088-2020《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（　）。
A、HTTP
B、TCP
C、UDP
D、TLCP 协议
答案：AD

76. 根据 GM/T 0088-2020《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（　）。
A、requestId 请求 ID
B、status 状态码
C、message 状态描述
D、timestamp 服务器响应时间
答案：ABCD

77. GM/T 0103-2021《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（　）。
A、单光子路径选择
B、相邻光子间时间间隔
C、激光相位噪声
D、放大自发辐射噪声
答案：ABCD

78. 以下属于 GM/T 0105-2021《软件随机数发生器设计指南》列举的通用熵源类型的是（　）。
A、系统时间
B、特定的系统中断事件
C、磁盘状态
D、人机交互输入事件
答案：ABCD

79. GM/T 0105-2021《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（　）
A、个性化字符串
B、额外输入
C、Nonce
D、设备序列号

答案：ABC

80. GM/T 0105-2021《软件随机数发生器设计指南》规定的健康测试包括（　）。
A、随意健康测试
B、连续健康测试
C、按需健康测试
D、上电健康测试
答案：BCD

81. 根据 GM/T 0078-2020《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。
A、采样时钟的频率
B、振荡源输出信号的抖动的标准差
C、振荡源的振荡时钟频率
D、采样时钟信号的抖动的标准差
答案：ABCD

82. GM/T 0078-2020《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（　）。
A、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
B、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
C、异或链级数越多，产生随机数效率越低
D、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
答案：ABCD

83. 在 GM/T 0013-2021《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
A、测试常量
B、变量
C、压力测试
D、集成测试
答案：AB

84. 在 GM/T 0012-2020《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。
A、产生非对称密钥
B、执行非对称加/解密
C、执行签名运算
D、执行验签运算
答案：ABCD

85. 在 GM/T 0082-2020《可信密码模块保护轮廓》中，安全威胁冒名的目的包括（　）。
A、身份标识
B、安全角色

C、受保护的功能
D、安全导入
答案：ABD

86. 根据 GM/T 0122-2022《区块链密码检测规范》，区块链中的交易记录包含（ ）等信息。
A、交易发起者
B、交易内容
C、交易接收者
D、交易发起者的用户签名
答案：ABCD

87. 根据 GM/T 0122-2022《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。
A、各个节点之间
B、各个区块之间
C、应用端与区块之间
D、应用端与节点之间
答案：AD

88. GM/T 0087-2020《浏览器密码应用接口规范 》中 SM4 算法不包括（ ）应用接口。
A、加密
B、解密
C、签名
D、验签
答案：CD

89. GB/T 38636-2020《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（ ）。
A、非对称密码算法
B、分组密码算法
C、数据扩展函数和伪随机函数
D、密码杂凑算法
答案：ABCD

90. GB/T 38636-2020《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。
A、预主密钥
B、客户端随机数
C、服务端随机数
D、常量字符串
答案：ABCD

91. 在 GM/T 0118-2022《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（　）。
A、用户证书
B、根证书
C、CA 中间证书
D、CRL
答案：ABCD

92. 在 GM/T 0118-2022《浏览器数字证书应用接口规范》中，检查证书状态的方式有（　）。
A、LDAP
B、CRL
C、OCSP
D、未定义获取证书状态的接口
答案：ABC

93. 根据 GM/T 0083-2020《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（　）。
A、差分能量分析
B、互信息能量分析
C、简单能量分析
D、简单电磁分析
答案：CD

94. 根据 GM/T 0083-2020《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（　）。
A、随机插入伪指令技术
B、伪轮运算技术
C、时钟随机化技术
D、乱序操作技术
答案：ABCD

95. GM/T 0084-2020《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（　）。
A、喷砂处理
B、时钟毛刺
C、电磁干扰
D、成像方法
答案：BCD

96. GM/T 0084-2020《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（　）。
A、气体分析
B、电压传感器
C、超声波传感器
D、压电片
答案：BCD

97. GM/T 0084-2020《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（　）。
A、手工材料移除
B、聚能切割
C、水刀加工
D、喷砂处理
答案：ACD

98. GB/T 39786-2021《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。
A、管理制度
B、人员管理
C、资金管理
D、应急处置
答案：ABD

99. 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（　）。
A、SSL
B、TLCP
C、IPSec
D、MPLS
答案：ABC

100. GB/T 39786-2021《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（　）。
A、第一级
B、第二级
C、第三级
D、第四级
答案：AB

101. 根据 GB/T 39786-2021《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。
A、发送方客户端到其网络出口 IPSec VPN 之前
B、发送方 IPSec VPN 与接收方 IPSec VPN 之间
C、重要数据在 ESP 协议保护下传输时
D、接收方网络出口 IPSec VPN 到应用服务器
答案：AD

102. 根据 GM/T 0116-2023《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（　）。
A、签署保密协议
B、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

C、签署测试授权书
D、工具测试避开业务运行高峰期
答案：ACD

103. 根据 GM/T 0116-2023《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。
A、密码产品的配置文件
B、密码产品调用指令
C、密码产品响应报文
D、密码产品的日志记录
答案：BC

104. 根据 GM/T 0116-2023《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（ ）。
A、自行模拟被测信息系统搭建测评环境获取测评数据
B、与被测单位协商、配合，生成必要的离线数据
C、告知被测单位风险后，接入被测系统获取真实数据
D、将该测评项做不适用处理
答案：ACD

105. 依据 GM/T 0009-2023《SM2 密码算法使用规范》，SM2 密文的数据结构中包含有（ ）。
A、一个随机的椭圆曲线点
B、一个用于校验的杂凑值
C、一个随机数
D、与明文长度相同的密文数据
答案：ABD

106. 依据 GM/T 0009-2023《SM2 密码算法使用规范》，长度为 32 字节的数据包括（ ）。
A、SM2 签名结果中的 R
B、Z 值
C、默认的用户标识
D、SM2 签名的输入数据
答案：ABCD

107. 下列哪些事件属于 GB/T 20986-2023《信息安全技术 网络安全事件分类分级指南》中定义的“数据安全事件”子类？（ ）
A. 数据投毒事件
B. 社会工程事件
C. 网页篡改事件
D. 数据泄露事件
答案：ABD

108. 下列哪些属于 GB/T 20986-2023《信息安全技术 网络安全事件分类分级指南》中“不可抗力事件”的子类？
A. 自然灾害事件
B. 社会安全事件
C. 设备设施故障事件
D. 公共卫生事件
答案：ABD

109. 依据 GM/T 0133-2024《关键信息基础设施密码应用要求》，下列关于密码运行安全事件应急处置相关要求描述正确的是（ ）。
A、应根据应急预案定期开展应急演练活动
B、应根据应急预案对已发生的密码运行安全事件实施分类分级处置，并形成事件处置记录
C、立根据法律、行政法规和国家有关规定要求，参与和配合保护工作部门开展的应急处置工作
D、应将应急预案纳人密码应用岗位人员的培训和考核内容
答案：ABCD

110. 依据 GM/T 0034-2014《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》，证书认证系统必须采用双证书,并建设双中心。这里的双证书指的是（ ）
A、签名证书
B、加密证书
C、公钥证书
D、私钥证书
答案：AB

111. 依据 GM/T 0001.1-2012《祖冲之序列密码算法 第 1 部分：算法描述》，ZUC 算法的整体结构包括哪三个主要部分？（ ）
A、线性反馈移位寄存器（LFSR）
B、比特重组（BR）
C、非线性函数 F
D、S 盒变换
答案：ABC

112. 依据 GM/T 0001.3-2012《祖冲之序列密码算法 第 3 部分：基于祖冲之算法的完整性算法》，完整性算法中，IV 的哪些部分是由 COUNT 直接填充的？（ ）
A、IV[0]
B、IV[1]
C、IV[2]
D、IV[3]
答案：ABCD

113. 某金融系统需加密传输敏感数据，选择 SM4 算法。依据 GM/T 0002-2012《SM4 分组密码算法》，以下关于 SM4 算法的说法正确的是（ ）。
A、SM4 是我国商用密码标准，属于分组密码算法

B、SM4 的分组长度为 128 位，密钥长度可为 128 位或 256 位
C、SM4 加密过程包含 32 轮非线性迭代运算
D、SM4 已通过对应的国际标准
答案：ACD

114. 依据 GM/T 0002-2012《SM4 分组密码算法》，下列关于 SM4 算法的 S 盒描述中，哪些是正确的？（ ）
A、S 盒是 8 比特输入 8 比特输出的置换表
B、S 盒的输出是通过查表得到的
C、S 盒的输入“EF”对应的输出为“84”
D、S 盒是动态生成的，每次加密不同
正确答案：ABC

115. 依据 GM/T 0003.1-2012《SM2 椭圆曲线公钥密码算法 第 1 部分：总则》，下列哪些属于 SM2 中定义的弱椭圆曲线？（ ）
A、超奇异曲线
B、异常曲线（Anomalous 曲线）
C、非奇异曲线
D、正规基表示的曲线
答案：AB

116. 依据 GM/T 0003.2-2012《SM2 椭圆曲线公钥密码算法 第 2 部分：数字签名算法》，SM2 数字签名算法中使用的辅助函数包括（ ）。
A、密码杂凑函数
B、随机数发生器
C、对称加密算法
D、消息认证码
答案：AB

117. SM2 曲线参数中，依据 GM/T 0003.5-2012《SM2 椭圆曲线公钥密码算法 第 5 部分：参数定义》，基点 G 的坐标(x_G, y_G)用于哪些操作？（ ）
A、生成用户公钥
B、计算用户杂凑值 Z_A
C、密钥派生函数 KDF
D、数字签名生成
答案：ABD

118. 依据 GM/T 0039-2024《密码模块安全检测要求》，密码模块的物理安全机制应满足以下哪些要求？（ ）
A、提供拆卸证据
B、允许非授权物理访问
C、在检测到拆卸行为后立即置零敏感安全参数
D、使用透明外壳以便观察内部结构
答案：AC

119. 依据 GM/T 0134-2024《密码模块安全设计指南》，密码模块的敏感安全参

数置零方式包括（　）。
A、手动置零
B、自动置零
C、逻辑置零
D、物理销毁
答案：AB

120. 依据 GM/T 0139-2024《信息系统密码应用安全管理体系》，密码应用方案中必须包含的内容包括（　）。
A、系统概述
B、密码应用设计
C、系统源代码
D、安全与合规性分析
答案：ABD

121. 依据 GM/T 0028-2024《密码模块安全要求》，下列哪些属于密码模块必须提供的服务？（　）
A、显示密码模块版本信息
B、执行自测试
C、提供操作系统升级服务
D、执行置零操作
答案：ABD

122. 以下哪些攻击类型被 GM/T 0028-2024《密码模块安全要求》附录 F 明确定义为“非入侵式攻击”？（　）
A、差分功耗分析（DPA）
B、故障注入攻击
C、电磁分析（DEMA）
D、物理拆卸探测
答案：AC

123. 对于安全三级的密码模块，依据 GM/T 0028-2024《密码模块安全要求》，手动建立的明文关键安全参数可以通过哪些方式进行输入或输出？（　）
A、以明文形式直接通过共享端口输入输出
B、经过加密后输入输出
C、使用可信信道输入输出
D、使用拆分知识过程输入输出
答案：BCD

124. 当密码模块的自测试失败时，依据 GM/T 0028-2024《密码模块安全要求》，模块应如何响应？（　）
A、进入错误状态
B、输出一个错误指示
C、停止执行任何密码操作
D、允许降级工作，提供有限服务
答案：ABC

125. GM/T 0028-2024《密码模块安全要求》中定义的“敏感安全参数”（SSP）包括哪些内容？（ ）
A、私钥、对称密钥
B、公钥证书
C、口令、PIN 等鉴别数据
D、自签名证书
答案：ABCD

126. 依据 GM/T 0080-2020《SM9 密码算法使用规范》，SM9 算法中，用户的公钥是如何确定的？（ ）
A、由 KGC 随机生成并分配给用户
B、由用户自己的身份标识（ID）通过公开的哈希函数和算法参数计算得出
C、是用户私钥所对应的椭圆曲线上的点
D、需要用户和通信方通过密钥协商协议临时产生
答案：BC

127. 依据 GM/T 0080-2020《SM9 密码算法使用规范》，以下哪些是 SM9 加密数据结构（SM9Cipher）中必然包含的组成部分？（ ）
A、加密类型（EnType），用于指明所使用的对称密码算法和模式
B、密钥封装值（C），用于传递加密密钥
C、明文的杂凑值（C3），用于验证解密结果的正确性
D、密文（CipherText），即对称加密算法对明文加密后的结果
答案：ACD

128. GM/T 0080-2020《SM9 密码算法使用规范》规定，在 SM9 密码体系中，密钥生成中心（KGC）负责生成并掌管哪些密钥？（ ）
A、签名主私钥（s_s）
B、加密主私钥（s_e）
C、用户签名私钥（d_s）
D、用户加密私钥（d_e）
答案：AB

129. 关于 SM9 的数字签名和验证过程，依据 GM/T 0080-2020《SM9 密码算法使用规范》，下列描述哪些是正确的？（ ）
A、签名过程需要用到签名者的用户签名私钥（d_s）
B、验证过程需要用到签名者的身份标识（ID）和签名主公钥（P_{pub-s}）
C、验证过程需要用到预处理得到的双线性对值 g_1
D、签名值中包含了对待签名消息本身进行杂凑后的结果
答案：ABCD

130. 根据 GM/T 0116-2023《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。
A、被测系统威胁分析结果
B、被测系统资产分析结果

C、被测系统存在的安全问题
D、已有安全措施情况
答案：ABCD

三、判断题 20
1. GB/T 39786-2021《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。
答案：对

2. GB/T 39786-2021《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。
答案：错

3. 根据 GM/T 0122-2022《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。
答案：对

4. GB/T 38636-2020《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，也需要重新协商安全参数。
答案：错

5. 在 GM/T 0005-2021《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。
答案：错

6. 在 GM/T 0078-2020《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。
答案：错

7. 根据 GM/T 0088-2020《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）服务器地址不能通过云服务器密码机管理接口 API 进行设置。
答案：错

8. 根据 GM/T 0104-2021《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。
答案：错

9. 在 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。
答案：对

10. 依据 GM/T 0134-2024《密码模块安全设计指南》，密码模块的“旁路能力”是必须支持的功能。

答案：错

11. 在 GM/T 0051-2016《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。
答案：错

12. GM/T 0037-2014《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。
答案：对

13. 在 GM/T 0058-2018《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。
答案：错

14. 根据 GM/T 0028-2024《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。
答案：错

15. 根据 GM/T 0039-2024《密码模块安全检测要求》，密码模块的密码边界至少应包含所有安全相关的算法、安全功能、过程和部件。
答案：对

16. 依据 GM/T 0134-2024《密码模块安全设计指南》，软件密码模块的物理端口必须明确说明。
答案：错

17. 依据 GM/T 0134-2024《密码模块安全设计指南》，密码模块的版本标识可以仅使用数字，无需包含字母或分段说明。
答案：错

18. GM/T 0139-2024《信息系统密码应用安全管理体系》规定，密码应用方案必须经过第三方评估并报送密码管理部门备案。
答案：对

19. 依据 GM/T 0139-2024《信息系统密码应用安全管理体系》，密码应用安全管理体系仅适用于第三级和第四级信息系统。
答案：错

20. 依据 GM/Z 4001-2013《密码术语》，假冒攻击指攻击者假冒用户，欺骗验证者的攻击方法。
答案：对

第三部分实操题 12

一、密码算法与安全挑战

1、非标准 RSA 密钥破解

题干描述：

在某一重要的量子通信项目中，开发团队为了提高加密速度，决定在系统中使用了一种非标准的 RSA 加密方案。不幸的是，由于错误的密钥生成方式，导致存在安全漏洞。

你的任务是破解出系统中的密钥并恢复重要的加密数据。

解题思路：

考察了基本的推导

$$h\,\mathrm{int}^e = m \bmod p$$

$$h\,\mathrm{int}^e - m = kp$$

$$p = \gcd(h\,\mathrm{int}^e - m, n)$$

解题脚本

```
from Crypto.Util.number import *
import gmpy2

# 已知的参数
n =
122307769217848803397686349366074305946210260978522734678909492722304314554419440203750498495438581598378674992078219279012782132141628374779279323560483520478724287077995018729807399806582903912854431760705676523361405189062684806859803088069487659359775136906616776443551770497701732269327498628572662532613392454661796594638975202231551924123746964994050127911973072094795875402789757737589307583669780348544660566750431392494828727432169614332089975702900409231479986376041832657945434209205687308884197298972252258463183207325026502672906549607135169825248779747819133787383398712608776411484988537857077334911231
hint =
157262789128867736405971209177655528471974319938371553549729029479461127394921793091766097590526660553642666686632438091911768071320130381311703023564980523567645585373349499905389148414618141628912491856704649508449912383247771843544095597424931703855542780938885012536046924210598830021570272117040080264865863221032742810051931908633326799929136499247061805757986334076492786162177374946023276483306870981765168618097955933046034558585382525033251962256904180969504280123
```

```
6578091370807041215185867922392599986045948008495354131824734361544270678281373
4547625465432726661805609400089666596442168438455903612453438
ee                                                                                =
5658876987486833758938184508651563723563244047343312760907949168527676895458754
91504478472729
ct                                                                                =
1126861323754053067914987733815570892924980059279810586057824919628122729083948
6481891971836075094645380571208325084492787969416710430847707712103213938087179
2270633165056787457486330409199374407084903887104180748575990601088900361894323
5987180247556761314506092654726145076816870346704008854339696051087555747677622
3203363977954176989285685842126761089114240490820415747103075106515843566365938
6909219332522673991255432502843095545978624066822506826578674844218769627158549
3847421194401983226799578266009110641713945394184953383387067222445360022721046
9970714097243232696328126272622408389926314390923152087411592270

# 字符串转为整数
m = bytes_to_long(b"Welcome_to_the_crypto_hack_world!!!")

e = 0x10001

# 计算 p
tmp = pow(hint, e, n) - m
p = gmpy2.gcd(tmp, n)   # 使用 gmpy2.gcd 函数
print(f"p = {p}")
print(f"p 是否为素数: {gmpy2.is_prime(p)}")

# 计算 q 和 phi(n)
q = n // p
phi = (p - 1) * (q - 1)

# 计算私钥 d
d = gmpy2.invert(ee, phi)

# 解密得到 flag
flag = pow(ct, d, n)

# 将整数 flag 转为字节并输出
print(f"解密后的 flag: {long_to_bytes(flag)}")
```

flag：flag{13ea90b1690b35dd638c519bad28b8a1}

二、逆向工程与密码破解

2、元宇宙密文解密挑战

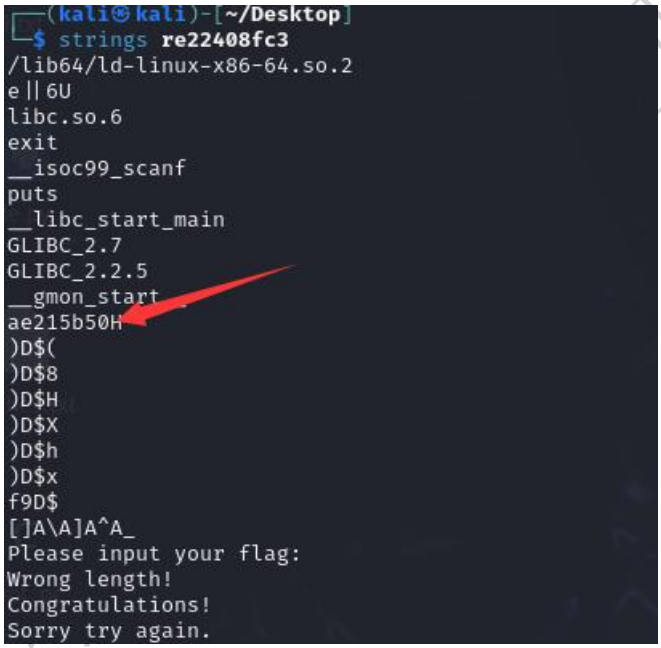
题干描述：

在某元宇宙虚拟交易平台上，所有的交易数据都经过简单的异或加密（每个字节与一个固定密钥进行异或操作），开发者用此方法保护交易记录，以防止敏感数据被第三方窃取。然而，由于使用的密钥较为简单，这种加密方式存在安全隐患。你截获了一段加密的虚拟交易数据，并且获得了一些文件。

你的任务是恢复交易数据的原始明文。

解题思路：

strings re22408fc3　发现密钥



1. 经分析后可知程序验证逻辑如下：

对输入的处理为：input -> xor ->enc

2. 分析出验证逻辑后就可以进行解密处理了，解密过程如下：

Enc -> xor -> input

```
import base64

enc_flag = [7, 9, 83, 86, 78, 85, 83, 84, 4, 6, 0, 8, 7, 82, 1, 5, 4, 85, 83, 5, 86, 83, 4, 5, 83, 80, 1, 1, 7, 7, 7, 86, 7, 0, 5, 83, 6, 31]
```

```
keys = ['ae215b50']

def xorpp_decrypt(enc, key):

    len_enc = len(enc)
    len_key = len(key)
    dec = []
    for i in range(len_enc):
        temp = (enc[i] ^ ord(key[i%len_key])) & 0xff
        dec.append(temp)

    return dec

def decrypto(enc_flag, keys):


    enc_flag = xorpp_decrypt(enc_flag, keys[0])

    return "".join(chr(elem) for elem in enc_flag)

def solve():
    flag = decrypto(enc_flag, keys)

    print(flag)

if __name__ == "__main__":
    solve()
```

运行后获得正确输入：

```
flag{7fdec292045e0a4c11525302e2ffe7b3}
```

3、信息通信的秘密分析

题干描述：

某公司在通信系统中开发了一种自定义的多层加密算法，用于保护高度机密的数据传输。你就职于该公司的安全审计部门，负责评估该加密系统的安全性。你拿到了一个可执行文件，初步分析表明，该文件实现了一种多层加密算法。它采用了非标准的 XTEA（Tiny

Encryption Algorithm）、循环移位操作，以及 AES-128 加密来加密用户的输入。为了验证用户输入是否正确，程序会将输入进行多层加密，最终与内置的密文进行比较。

你的任务是通过逆向分析和密码学知识，找到正确的输入，完成解密流程。

解题思路：

1.找到 main 函数，继续分析可知关键函数功能

循环移位

```
char __fastcall sub_140001E80(char *a1)
{
  char v2; // cl
  char result; // al

  *a1 = (2 * *a1) | (*a1 >> 7) & 1;
  a1[1] = (2 * a1[1]) | (a1[1] >> 7) & 1;
  a1[2] = (2 * a1[2]) | (a1[2] >> 7) & 1;
  a1[3] = (2 * a1[3]) | (a1[3] >> 7) & 1;
  a1[4] = (2 * a1[4]) | (a1[4] >> 7) & 1;
  a1[5] = (2 * a1[5]) | (a1[5] >> 7) & 1;
  a1[6] = (2 * a1[6]) | (a1[6] >> 7) & 1;
  a1[7] = (2 * a1[7]) | (a1[7] >> 7) & 1;
  a1[8] = (2 * a1[8]) | (a1[8] >> 7) & 1;
  a1[9] = (2 * a1[9]) | (a1[9] >> 7) & 1;
  a1[10] = (2 * a1[10]) | (a1[10] >> 7) & 1;
  a1[11] = (2 * a1[11]) | (a1[11] >> 7) & 1;
  a1[12] = (2 * a1[12]) | (a1[12] >> 7) & 1;
  a1[13] = (2 * a1[13]) | (a1[13] >> 7) & 1;
  a1[14] = (2 * a1[14]) | (a1[14] >> 7) & 1;
  v2 = a1[15];
  result = 2 * v2;
  a1[15] = (2 * v2) | (v2 >> 7) & 1;
  return result;
}
```

非标准 xtea，循环次数和魔法常量以及移位常量发生变化

```
v2 = a1[1];
v3 = a2[2];
v4 = a2[1];
v5 = (*a2 ^ (v2 + ((32 * v2) ^ (v2 >> 6)))) + *a1;
v6 = a2[3];
v7 = ((v3 + 0x33151655) ^ (v5 + ((16 * v5) ^ (v5 >> 5)))) + v2;
v8 = ((v4 + 857019989) ^ (v7 + ((32 * v7) ^ (v7 >> 6)))) + v5;
v9 = ((v4 + 1714039978) ^ (v8 + ((16 * v8) ^ (v8 >> 5)))) + v7;
v10 = ((v3 + 1714039978) ^ (v9 + ((32 * v9) ^ (v9 >> 6)))) + v8;
v11 = ((*a2 - 1723907329) ^ (v10 + ((16 * v10) ^ (v10 >> 5)))) + v9;
v12 = ((v6 - 1723907329) ^ (v11 + ((32 * v11) ^ (v11 >> 6)))) + v10;
v13 = ((v6 - 866887340) ^ (v12 + ((16 * v12) ^ (v12 >> 5)))) + v11;
v14 = ((*a2 - 866887340) ^ (v13 + ((32 * v13) ^ (v13 >> 6)))) + v12;
v15 = ((v4 - 9867351) ^ (v14 + ((16 * v14) ^ (v14 >> 5)))) + v13;
v16 = ((v4 - 9867351) ^ (v15 + ((32 * v15) ^ (v15 >> 6)))) + v14;
v17 = ((*a2 + 847152638) ^ (v16 + ((16 * v16) ^ (v16 >> 5)))) + v15;
v18 = ((v3 + 847152638) ^ (v17 + ((32 * v17) ^ (v17 >> 6)))) + v16;
v19 = ((v6 + 1704172627) ^ (v18 + ((16 * v18) ^ (v18 >> 5)))) + v17;
v20 = ((v6 + 1704172627) ^ (v19 + ((32 * v19) ^ (v19 >> 6)))) + v18;
v21 = ((v3 - 1733774680) ^ (v20 + ((16 * v20) ^ (v20 >> 5)))) + v19;
v22 = ((*a2 - 1733774680) ^ (v21 + ((32 * v21) ^ (v21 >> 6)))) + v20;
v23 = ((v4 - 876754691) ^ (v22 + ((16 * v22) ^ (v22 >> 5)))) + v21;
v24 = ((v4 - 876754691) ^ (v23 + ((32 * v23) ^ (v23 >> 6)))) + v22;
*a1 = v24;
result = (unsigned int)(v6 - 19734702);
a1[1] = (result ^ (v24 + ((16 * v24) ^ (v24 >> 5)))) + v23;
return result;
```

AES-128，查看密钥长度为 16 字节

```
.data:0000000140006074                  align 8
.data:0000000140006078 aDfb8007c773561 db 'dfb8007c773561da',0 ; DATA XREF: main+169↑o
.data:0000000140006089                  align 20h
```

经分析后可知程序验证逻辑如下：

对输入的处理为：将输入 32 字节转成 16 字节 hex 模式，然后对其逐字节进行循环移位，非标准 xtea 加密和 AES 加密，最终得到密文和程序内置密文数据进行比较

分析出验证逻辑后就可以进行解密处理了，解密过程如下：

Enc -> AES -> xtea ->循环移位 -> input

运行后获得正确输入：

```
decaec9d25889199865401fb84cd8a7c
```

三、密码应用与协议安全

4、金融密码机的秘密通信

题干描述：

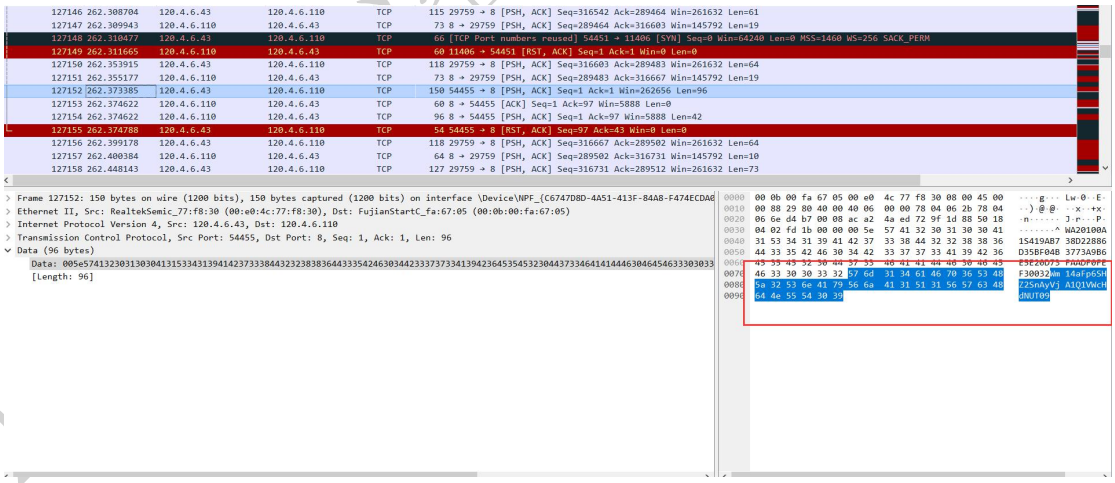
某金融云平台遭受了不明黑客组织攻击。经分析发现，异常流量是攻击者利用中间人攻击（MITM）技术，对银行金融密码机与核心系统之间的加密通信进行探测和截获。这台金融密码机负责执行关键的加密、解密和密钥管理操作，是银行处理大额交易和敏感金融信息的核心设备。攻击者成功捕获了密码机的一段流量包，并通过分析其中的通信数据，窃取操作员传输的敏感信息。为防止潜在的数据泄露和经济损失，银行迫切需要解密这些流量，识别并确认其中的有效字符。

你的任务对捕获的流量包进行分析，还原这些字符的原始内容。

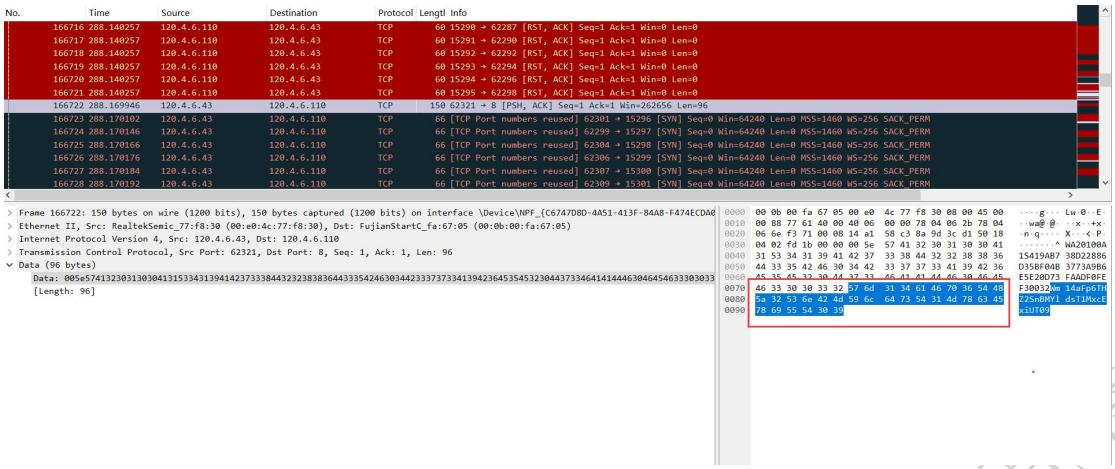
解题思路：

分析流量包，发现特殊的 4 段 hex 值 解码两次 base64

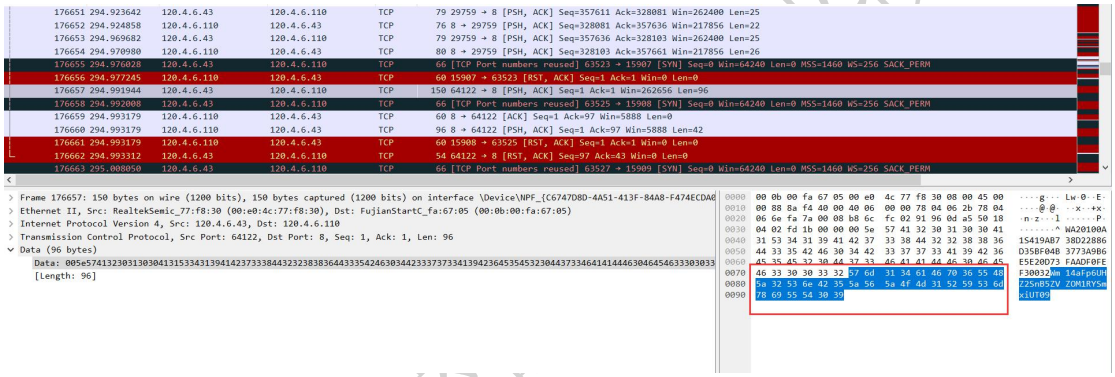
57 6D 31 34 61 46 70 36 53 48 5A 32 53 6E 41 79 56 6A 41 31 51 31 56 57 63 48 64 4E 55 54 30 39



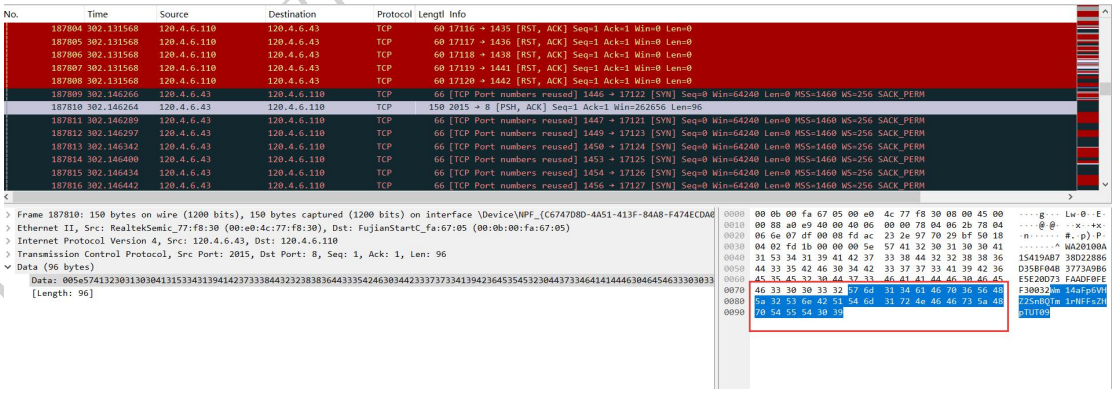
57 6D 31 34 61 46 70 36 54 48 5A 32 53 6E 42 4D 59 6C 64 73 54 31 4D 78 63 45 78 69 55 54 30 39

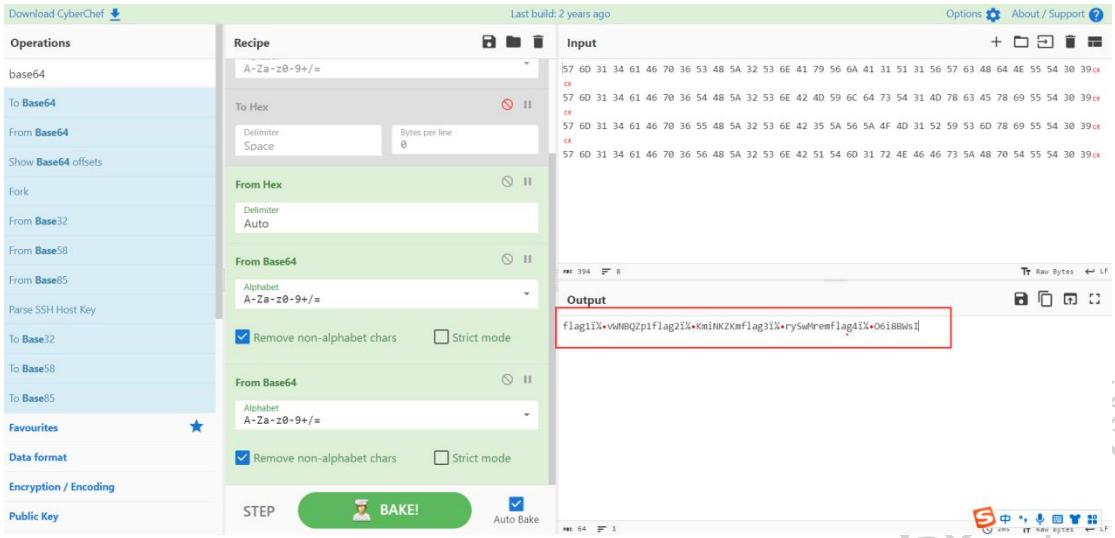


57 6D 31 34 61 46 70 36 55 48 5A 32 53 6E 42 35 5A 56 5A 4F 4D 31 52 59 53 6D 78 69 55 54 30 39



57 6D 31 34 61 46 70 36 56 48 5A 32 53 6E 42 51 54 6D 31 72 4E 46 46 73 5A 48 70 54 55 54 30 39





flag1：vWNBQZp1

flag2：KmiNKZKm

flag3：rySwMrem

flag4：O6i8BWsI

flag{vWNBQZp1KmiNKZKmrySwMremO6i8BWsI}

5、API 数据加密解密挑战

题干描述：

你是一名网络安全分析师，最近，你在一次社交媒体安全监测平台的告警中，发现了一个可疑的 API 接口。该接口返回了一些加密的数据，经过分析，你认为这些数据可能是某种敏感信息。你还发现了服务端的部分加密代码，推测这些数据经过一定的加密规则生成。明文: "Charlie" -> 密文: 910732376661017344　密文: 16552436225337

你的任务是分析该加密逻辑，编写解密代码，并通过解密得到一

个新的密文对应的明文，从而还原 API 接口传递的实际内容。

解题思路：

1、理解加密代码：

通过阅读加密代码，选手可以看到 generate_parameters(index) 函数用于生成两个参数 a 和 b。

参数 a 和 b 的生成规则是根据索引 index 进行的简单数学运算，因此只要知道 index，就可以重新生成相同的 a 和 b。

2、分析加密操作：

加密过程为：先将明文转化为整数 m，然后计算 (m * a) + b 得到密文 cipher。

选手需要理解：加密过程主要是用 a 进行放大（乘法），再用 b 进行偏移（加法）。

3、推导解密方法：

解密就是要反向操作，恢复出 m。

从密文 cipher 得到原始整数 m 的步骤是：先从 cipher 中减去 b，然后将结果除以 a。公式为：

m = (cipher - b) // a

4、根据加密代码编写解密代码：

选手要重新使用 generate_parameters(index) 函数，生成与加密时相同的 a 和 b。

利用上面的反向公式来计算原始的 m，然后将 m 转换回字符串得到明文。

5、示例解密过程：

假设 index = 4（这是从新的密文的情况推断出来的），可以通过 generate_parameters(4) 得到 a 和 b。

对 新密文: 16552436225337 进行解密：

通过 a, b = generate_parameters(4) 获取参数。

使用 m = (16552436225337 - b) // a 得到原始整数 m。

将整数 m 转换回字节形式，再解码成字符串，即可得到明文。

EXP

```
from Crypto.Util.number import long_to_bytes

def generate_parameters(index):
    # 重新生成 a 和 b
    a = (index * 5 + 9) * 2
    b = (index * 3 + 7)
    return a, b

def decrypt_message(ciphertext, index):
    # 逆向操作：先获取 a 和 b
    a, b = generate_parameters(index)

    # 解密步骤：减去 b，然后除以 a，得到原始的 m
    m = (ciphertext - b) // a

    # 转换回原始的明文
    return long_to_bytes(m).decode()

# 使用新的密文进行解密
new_ciphertext = 16552436225337
index = 4

# 获取解密后的明文
decrypted_message = decrypt_message(new_ciphertext, index)
print("解密后的明文:", decrypted_message)
```

flag{Bravo}

四、密码与安全杂项挑战

6、分布式存储系统密钥泄露

题干描述：

在当前分布式存储系统广泛应用的环境下，许多公司依赖分布式存储系统来处理和存储海量数据。这些系统多使用 RSA 加密来保护传输和存储过程中的敏感信息。在某网络安全审计中，研究人员发现多个分布式存储节点在使用相同的模数 n，但使用了不同的公钥指数来加密数据。这一设计上存在缺陷。

你的任务是破解加密的数据，获取系统中存储的敏感信息。

解题思路：

1、确定共模攻击的条件：

- 两个加密数据 c1 和 c2 是使用相同的模数 n 但不同的公钥指数 e1 和 e2 加密的同一明文。由于模数相同，这种情况下可以使用 共**模攻击**。

2、构建方程：

RSA 加密公式为：$c1 = m^{e1} \mod n$，$c2 = m^{e2} \mod n$ 其中，m 是明文，c1 和 c2 是密文，e1 和 e2 是两个不同的公钥指数，n 是模数。

3、应用中国剩余定理（CRT）：

根据 共模攻击，当相同模数下使用不同指数加密同一明文时，可以使用 中国剩余定理 来破解明文。其步骤为：

使用 e1 和 e2 作为加密指数，构建方程组，运用 扩展欧几里得算法 计算出一个线性组合，使得能够通过解密方程推导出明文。

（1）计算逆元：

通过 扩展欧几里得算法 计算出 e1 和 e2 的线性组合，找到相应的系数，使得可以通过逆模运算恢复明文。

（2）还原明文：

通过公式和中国剩余定理的结果计算出原始明文 m，从而破解加密的密文，获得原始的敏感信息（flag）。

EXP

```
#coding:utf-8
import gmpy2
import libnum

n=
161492506884166833433517609377161674255367889444964329085254933192280933288174016159403846732995683464537582153865439775385985507113637195002581323940901351529421413536755944252076579924468492236423535800520655077434820879199455394780766066733997339591381637890322185024405004208020732157100631980203839179078757755199610850261689227811513939380618096540465885798483259587860673543738338123577737766334069502862964769514115135674532010057059370062051862094330482913069710366202420367134157584132023425662209381931413665104273024963051198696866053559651143274839777358212657520435463266952424497868640876195721646459691
e1= 2333
c1=
131042593001214575843716650803494599335711306286351993108868647495840369947313294090657547359988464357930455477313835423293905386303612018520297909522864209052584533737403870693193231991536328762829791345138700681248847774902892771927093003395749580688617912409911659037463521831429821468645457726927191506665582694561590809379988582766952927909960912908121279156186609889089417551042247932067415699204990505602627762397673490832509384326431771166782603844695840776901118874643667915323885660427389599123101301783620844906536347097628042479786546479275401118504453631461403623619154423863541925534478752042933161553421
e2= 23333
c2=
933216833359588741907248986434456797086635254018408521207181059334053768031674585172801059693546082966499148936778928727243128099213242449459717068317133685834595966042287248325543767968541485928404010347750561034524210995223980767892805781205953518908392292950760538527176810017573993572093529081873714673714883422564086688950841946066808915982409484062711455428861226374456502997733346415218391
```

```
11815956509830731990806046389045169406717866354552964641626430395803527582171324547995818863298696776424275401762731849747424328732318923836486509127067461797172007060045785555249527098923185712881806184008672748325755412

#共模攻击
#共模攻击函数
def rsa_gong_N_def(e1,e2,c1,c2,n):
    e1, e2, c1, c2, n=int(e1),int(e2),int(c1),int(c2),int(n)
    s = gmpy2.gcdext(e1, e2)
    s1 = s[1]
    s2 = s[2]
    if s1 < 0:
        s1 = - s1
        c1 = gmpy2.invert(c1, n)
    elif s2 < 0:
        s2 = - s2
        c2 = gmpy2.invert(c2, n)
    m = (pow(c1,s1,n) * pow(c2 ,s2 ,n)) % n
    return int(m)
m = rsa_gong_N_def(e1,e2,c1,c2,n)
print(m)
print(libnum.n2s(int(m)))
```

```
25114135108420821919577162745132664605273806686171610108l3
b'flag{smbzhendehaohaowan}'
```

flag{smbzhendehaohaowan}

五、编码转换（encoded）

7、滴答 7

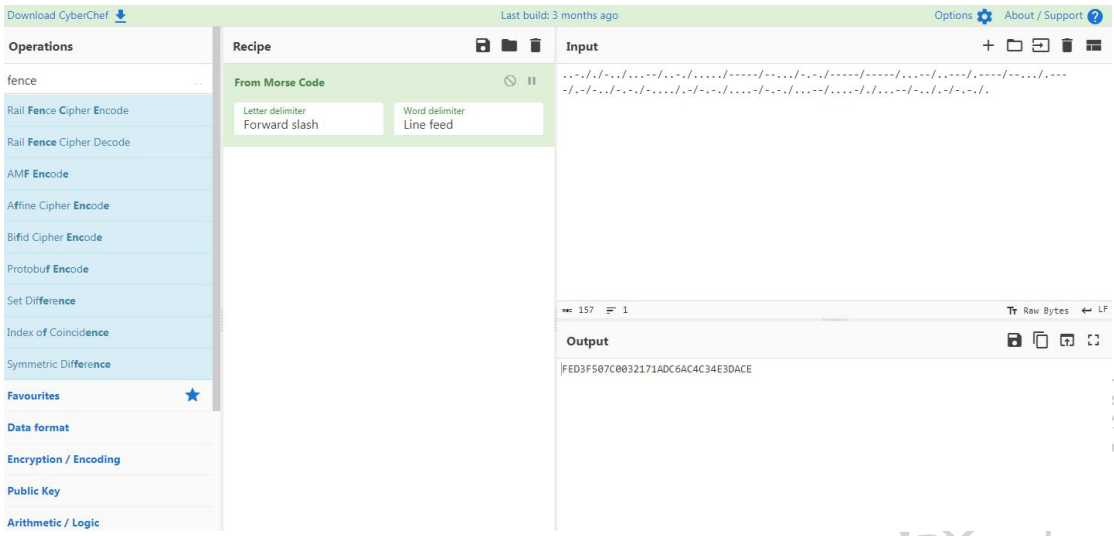
题干描述：

超级变换 滴答 8 5

..-././-../...--/..-./...../-----/--.../-.-./-----/-----/...--/..---/.----/--.../.----/.-/-../-.-./-..../.-/-.-./....-/-.-./...--/....-/./...--/-../.-/-.-./.

解题思路：

根据题目提示 滴答为摩斯密码



尝试 8 为栅栏密码栏数

5 为 md5

flag：flag{20230701}

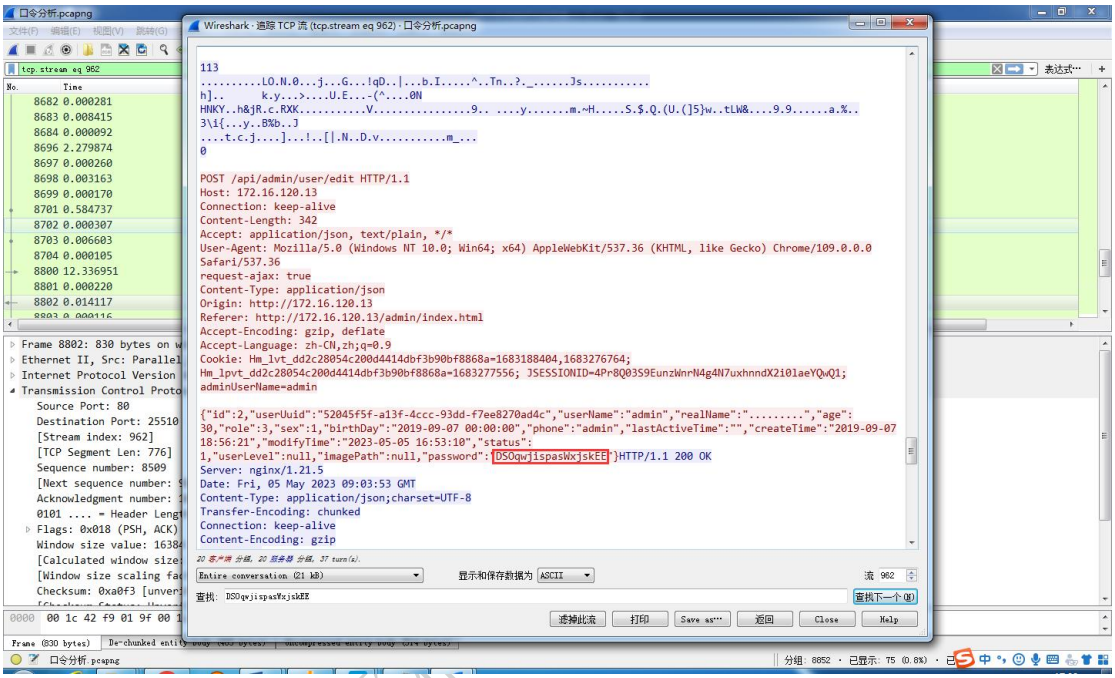
六、流量分析（analysis）

8、简简单单

题干描述：

小王是某系统管理员，近期发现系统频发出现异常，小王决定修改后台管理员口令，没想到的是修改口令的过程被攻击者采用流量监听的方式截取了数据包。你能分析出小王修改之后的口令是什么吗？

解题思路：



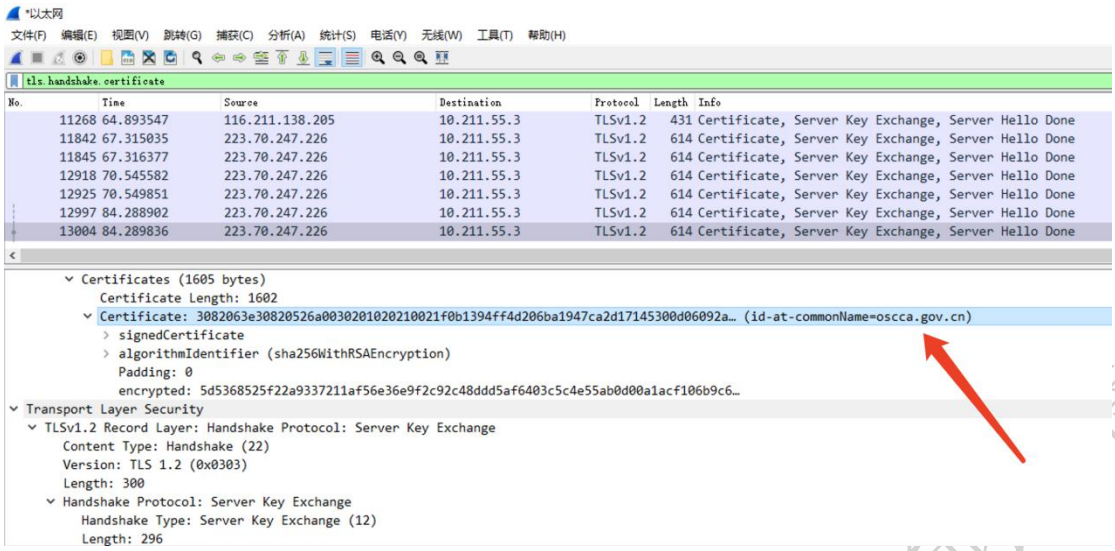
flag：flag{DSOqwjispasWxjskEE}

9、 oscca

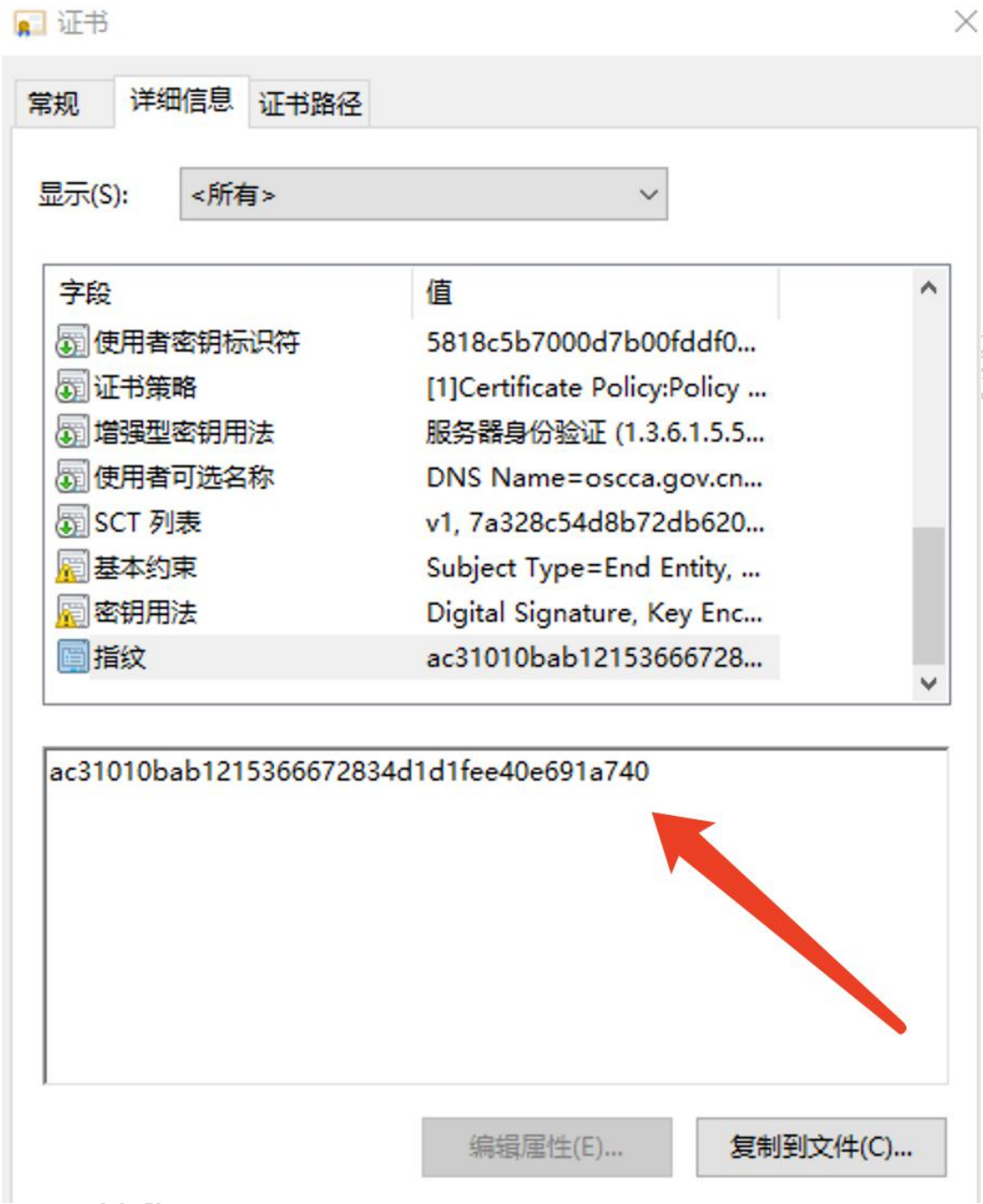
题干描述：

张三在国家密码管理局（oscca.gov.cn）搜索资料的时候被黑客抓包了，你能从中找到张三的证书指纹吗？

解题：



导出成 cer



flag：flag{ac31010bab1215366672834d1d1fee40e691a740}

七、密码破译（decipher）

10、 AES

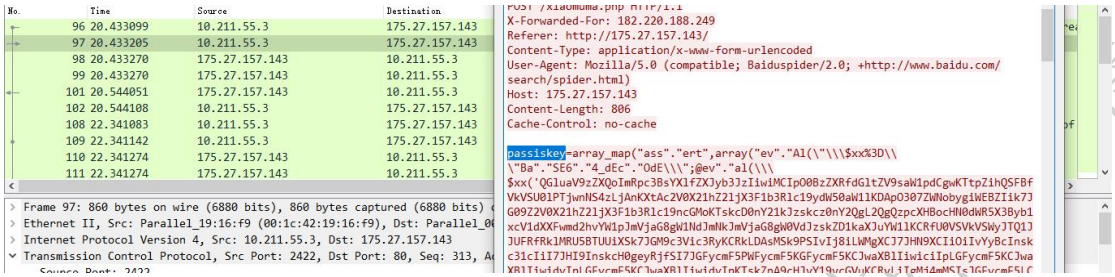
题干描述：

某安全专家在分析网络攻击日志的时候，发现某重要信息被攻击者窃取，由于时间紧任务重，你能帮助他一起分析出对应的明文信息

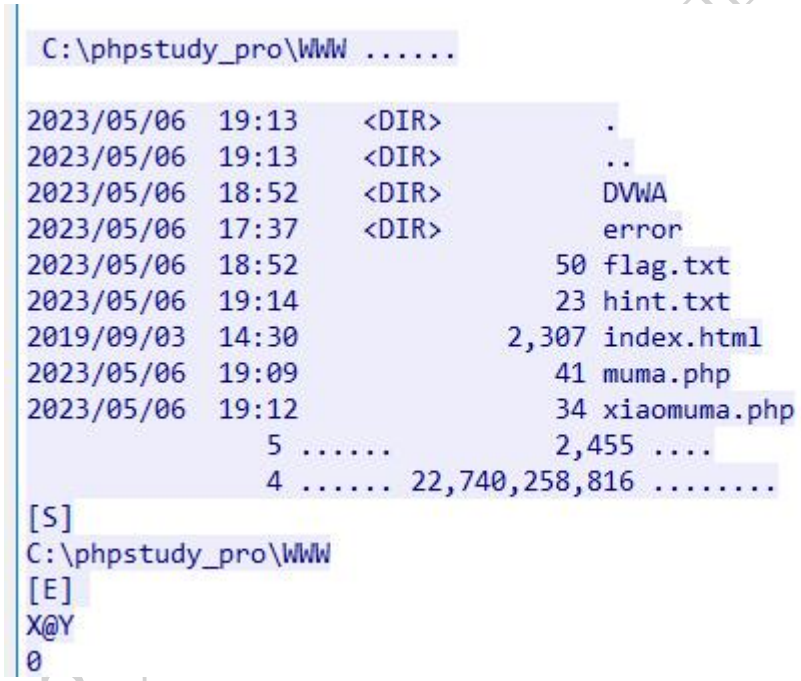
吗？

解题思路：

首先发现黑客上传了一个 xiaomuma.php 并连接，连接口令为 passiskey，暗示了后面的 AES 的 key 就是木马的 key



黑客执行了 dir，typ 了 flag.txt



```
%2BJjEiLCRhcnJheSwkcGlwZXMpOyRyZXQ9c3RyZWFtX2dldF9jb250ZW50cygkcGlwZXNb
NfY2xvc2UoJGZwKTtwcmludCAkcmV0OztlY2hvKCJYQFkiKTtkaWUoKTs%3D'));\");"))
200 OK
Server: nginx/1.15.11
Date: Sat, 06 May 2023 11:15:26 GMT
Content-Type: text/html; charset=UTF-8
Transfer-Encoding: chunked
Connection: keep-alive
X-Powered-By: PHP/5.6.9

58
X@Yflag{IvLRd8zH07ydznltDJAzf3M1rzLOc/HWRj0FHscprb0=}[S]
C:\phpstudy_pro\WWW
[E]
X@Y
0
```

发现了 flag，但是里面是加密的

查看 hint.txt

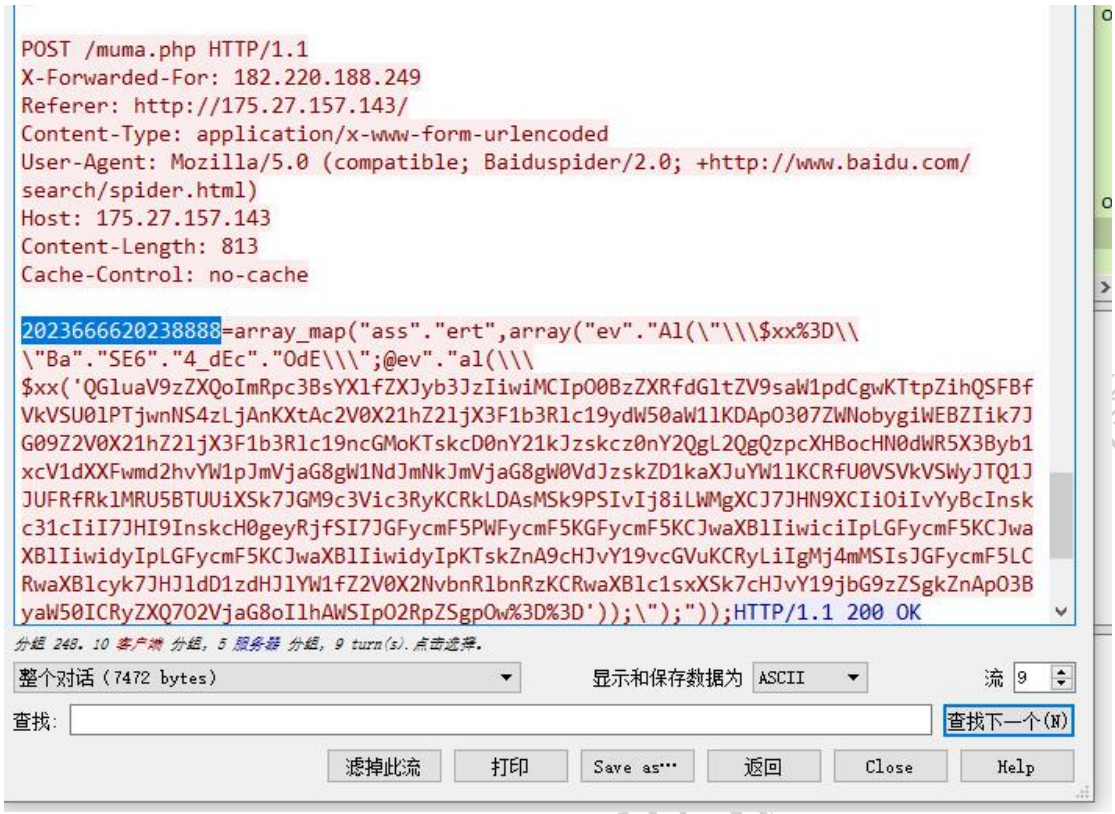
```
200 OK
Server: nginx/1.15.11
Date: Sat, 06 May 2023 11:15:31 GMT
Content-Type: text/html; charset=UTF-8
Transfer-Encoding: chunked
Connection: keep-alive
X-Powered-By: PHP/5.6.9

3d
X@Ywhereispass?
whosekey?[S]
C:\phpstudy_pro\WWW
[E]
X@Y
0
```

Hint 里面提问，哪里有 pass，对应的是 passiskey，下面一句 whosekey，对应的是谁的 key

一般人会用小木马的 key 解，但是这里不对，要仔细分析数据包，后面又传了木马

应该用木马的 key



2023666620238888

最终获得 flag

flag：flag{smb!_smb@_smb#}

八、算法攻击（**algorithm**）

11、 BOOM

题干描述：

猜猜明文

data = boomboom_is_****

6141ec30cded7beed78bec6e8ee

Flag{data}

解题思路：

看到了题目里的 boom 猜到是爆破，看密文长度接近 32 位，猜测是 MD5 明文爆破

脚本：

```
#coding: utf-8
import hashlib
dic = '0123456789abcdefghijklmnopqrstuvwxyzABCDEFGHIJKLMNOPQRSTUVWXYZ-'

for a in dic:
    for b in dic:
        for c in dic:
            for d in dic:
                # flag = ' boomboom_is ' + str(a) + str(b) + + str(c) + + str(d)
                flag = 'boomboom_is_'+a+b+c+d
                md5 = hashlib.md5(flag.encode('utf-8')).hexdigest()
                if md5[:27] == "6141ec30cded7beed78bec6e8ee":
                    print(flag)
print("over")
```

flag：flag{boomboom_is_e4sy}

12、 RSA_Compliant_correct_effective

题干描述：

RSA 也要使用合规正确有效

n=
21561333477383193077795753055605414562530479072352973956589155197382407568314408974492676890827604693350178538804311885473482202424344439676592768146360763826

37864026885098695104673487242270732322082149874845376292932909888683168556016301696735973644868727606517683757459425174525269779630105965147974517182249701598650568089037525573823344639970450296414734643981466750280233401020181724115626131198279451242702168692265894615019615309697125900466890393578169471631963581609663160455508890541176044924330523201325459025014045860850865757965303932465272096407678612420306229942459846028250597555441949412562853169025 1

e= 3

c=

22173447507982376688156979538651365127718717408254708273429468160937796402331993400342801177908930493125564766470993675009332203819905251209879573948716425241792160160466565588293005092146617583798171621802120865068745215170253312675506054353534497233662792122017254745414 13

解题思路：

考察 RSA 低指数攻击

```
import gmpy2
import libnum

def de(c, e, n):
    k = 0
    while True:
        mm = c + n*k
        result, flag = gmpy2.iroot(mm, e)
        if True == flag:
            return result
        k += 1
e= 3
n=
c=

m=de(c,e,n)
print(m)
print(libnum.n2s(int(m)).decode())
```

flag：flag{181808cf72bf134307de57aa78040e0f}