2026年江苏省密码行业
职业技能竞赛题库
（理论+实操）

竞赛组委会

2026年8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：GM/T 0111-2021《区块链密码应用技术要求》、GM/T 0129-2023《SSH 密码协议规范》、GB/T 17964-2021《信息安全技术 分组密码算法的工作模式》、GM/T 0021-2023《动态口令密码应用技术规范》、GB/T 45654-2025《网络安全技术 生成式人工智能服务安全基本要求》、GB/T 46800-2025《生成式人工智能技术应用社会影响评估指南》、GB/T 17901.1-2020《信息技术 安全技术 密钥管理 第 1 部分：框架》、GB/T 17901.3-2021《信息技术 安全技术 密钥管理 第 3 部分：采用非对称技术的机制》、GM/T 0074-2019《网上银行密码应用技术要求》、GM/T 0025-2023《SSL VPN 网关产品规范》、GM/T 0108-2021《诱骗态 BB84 量子密钥分配产品技术规范》、GM/T 0032-2014《基于角色的授权管理与访问控制技术规范》、GM/T 0043-2024《数字证书互操作检测规范》、GM/T 0057-2018《基于 IBC

技术的身份鉴别规范》、GM/T 0112-2021《PDF 格式文档的密码应用技术要求》、GM/T 0095-2020《电子招投标密码应用技术要求》、GM/T 0070-2019《电子保单密码应用技术要求》、GM/T 0124-2022《安全隔离与信息交换产品密码检测规范》、GM/T 0111-2021《区块链密码应用技术要求》、GM/T 0119-2022《PLC 控制系统及 PLC 控制器密码应用技术规范》、GM/T 0043-2024《数字证书互操作检测规范》、GM/T 0106-2021《银行卡终端产品密码应用技术要求》、GM/T 0023-2023《IPSec VPN 网关产品规范》、GM/T 0101-2020《近场通信密码安全协议检测规范》、GM/T 0065-2019《商用密码产品生产和保障能力建设规范》、GM/T 0066-2019《商用密码产品生产和保障能力建设实施指南》、GM/T 0126-2023《HTML 密码应用置标语法》、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 215

一、密码法律法规 65

一、单选题 40

1. 商用密码用于保护哪类信息（　　）
A. 国家秘密信息
B. 绝密级信息
C. 不属于国家秘密的信息
D. 所有信息
答案：C

2. （　　）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. 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. 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、密码资源管理平台登录口令
C、抗量子密码
D、税票防伪标识符的加密算法
答案：B

5. 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

6. 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

7. （　）不属于《中华人民共和国密码法》中规定的国家机关和涉及密码工作的单位。
A.某市公安局
B.承担密码管理职责的企业
C.承担密码管理职责的事业单位
D.某市密码管理局
答案：A

8. 某金融机构在日常业务中使用了不属于国家秘密的信息。根据《中华人民共和国密码法》的规定，该金融机构应当使用（　）类型的密码。
A.核心密码
B.普通密码
C.商用密码
D.军用密码
答案：C

9. 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

10. 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

11. 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

12. 《商用密码管理条例》是一部专门规范商用密码管理的重要行政法规，根据条例中描述的，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

13. 某机关工作人员小张被安排参加密码安全教育培训。根据《中华人民共和国密码法》的规定，密码安全教育被纳入（　　）教育体系。
A.纳入国民教育体系和高等教育体系
B.仅纳入公务员教育培训体系
C.纳入国民教育体系和公务员教育培训体系
D.仅纳入高等教育体系
答案：C

14. 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

15. 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

16. 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

17. 某企业拟通过海外代理商在境外销售该软件，依法应当办理（　　）手续？
A.自由出口，仅需在海关报关时声明含加密功能即可
B.必须将该软件的源代码全部销毁方可出口
C.依法申请出口许可，由国务院商务主管部门会同国家密码管理部门实施出口管制

D.向世界贸易组织提交技术说明，获批准后出口
答案：C

18. 某大型互联网票务平台被依法认定为关键信息基础设施运营者，在连续两年的安全监督检查中，均被发现未依法开展商用密码应用安全性评估。密码管理部门初次针对该违法行为作出处理时，首先可采取的措施是（　　）。
A.直接对该平台处以五十万元罚款
B.责令改正，给予警告
C.通报通信管理部门，暂时关闭其网站
D.吊销其营业执照
答案：B

19. 某互联网企业开发了一款手机加密相册 App，该 App 采用特定算法对用户照片进行加密保护和安全认证。关于该 App 是否属于《中华人民共和国密码法》所界定的“密码”，以下说法正确的是（　　）。
A.不属于，因为“密码”仅指硬件加密设备
B.属于，因为其采用特定变换方法对信息进行加密保护和安全认证
C.不属于，因为该 App 未取得商用密码产品认证证书
D.属于，但仅当用于保护国家秘密时才可以称为“密码”
答案：B

20. 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

21. 某地市级人民政府拟将密码工作纳入本地发展规划。根据《中华人民共和国密码法》的规定，下列关于密码工作经费保障的说法正确的是（　　）
A.密码工作所需经费由各使用单位自行解决
B.密码工作所需经费列入本级财政预算
C.密码工作所需经费由中央财政统一拨付
D.密码工作所需经费通过社会募集方式解决
答案：B

22. 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.安全风险评估、安全风险评估、事件报告、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

23. 《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

24. 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

25. 《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

26. 某公民从境外购买了一台个人使用的加密手机，该手机采用的商用密码属于大众消费类产品范畴。根据《中华人民共和国密码法》的规定，关于该手机所采用商用密码的进口管理，下列哪一说法是正确的（　）。
A.必须取得进口许可后方可进口
B.不实行进口许可制度
C.由海关自由裁量是否放行
D.仅需向密码管理部门备案即可
答案：B

27. 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

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. 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

32. 某科技自媒体发文举报称，一家社交软件公司在其即时通讯产品中未经批准违规使用商用密码。省密码管理部门依法应当首先采取的行动是（　　）。
A.直接约谈公司法人代表，要求其立即下架产品
B.告知举报人这属于民事纠纷，建议向法院起诉
C.对举报内容进行登记，组织开展调查核实，根据核实结果依法处理
D.以举报不实为由不予受理，因为商用密码无需监管
答案：C

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. 在《商用密码管理条例》中，下列对于“商用密码”的描述正确的是（　）。
A.商用密码是指对涉及国家秘密的信息进行加密保护所使用的密码技术和密码产品
B.商用密码是指采用特定变换的方法对不属于国家秘密的信息等进行加密保护、安全认证的技术、产品和服务
C.商用密码仅指密码产品，不包括技术和服务
D.商用密码是指可以商用的密码
答案：B

35. 根据《商用密码管理条例》规定，关于商用密码检测认证，下列选项中表述正确的是（　　）。
A.商用密码涉及网络安全，商用密码活动必须接受商用密码检测认证
B.通过商用密码检测认证后，从事商用密码相关活动将不再需要许可
C.商用密码检测认证机构应当经国家密码管理部门认定
D.商用密码检测认证机构应当取得相应资质
答案：D

36. 某商用密码标准制定工作组成员在参与标准制定过程中，需要明确各类标准的制定主体和相互关系。根据《商用密码管理条例》，以下表述错误的是（　　）。
A.国务院标准化行政主管部门和国家密码管理部门依据各自职责，组织制定商用密码国家标准、行业标准
B.国家密码管理部门对商用密码团体标准的制定进行规范、引导和监督
C.其他领域的标准涉及商用密码的，应当与商用密码国家标准、行业标准保持协调
D.商用密码团体标准的制定需要自行监督
答案：D

37. 根据《商用密码管理条例》规定，取得商用密码认证机构资质，应当符合相应程序，下列选项中表述正确的是（　　）。
A.应当向国家密码管理部门提出书面申请
B.国家密码管理部门审查资质申请时，应当征求国务院市场监督管理部门意见
C.应当向国务院市场监督管理部门提出书面申请
D.国务院市场监督管理部门应当独立审查资质申请
答案：C

38. 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

39. 根据《商用密码管理条例》规定，关于商用密码标准化，下列选项中表述正确的是（　　）。
A.商用密码中国标准不能与国外标准转化

B.国家密码管理部门独立负责制定商用密码国家标准
C.国家密码管理部门应当对商用密码标准的实施进行监督检查
D.为促进商用密码技术发展，其他领域的标准如果涉及商用密码，可以不与商用密码行业标准保持协调
答案：B

40. 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

二、多选题 13

1. 某大型军工企业集团正在建设一套涉密信息系统，用于存储和处理国家秘密信息。该集团信息安全部门在制定密码应用方案时，需要依据《中华人民共和国密码法》的相关规定进行规划。以下关于该涉密信息系统密码使用的说法，正确的有（　　）
A.该信息系统应当使用核心密码或普通密码进行加密保护和安全认证
B.核心密码保护信息的最高密级为绝密级，普通密码保护信息的最高密级为机密级
C.该企业可以自主选择商用密码产品来保护系统中的国家秘密信息
D.核心密码、普通密码属于国家秘密，由密码管理部门实行严格统一管理
答案：ABD

2. 某高校计算机学院正在组织学生学习《中华人民共和国密码法》，教师在课堂上讲解密码的分类。以下关于密码分类的说法，正确的有（　　）
A.国家对密码实行分类管理
B.密码分为核心密码、普通密码和商用密码
C.核心密码、普通密码属于国家秘密
D.商用密码用于保护不属于国家秘密的信息
答案：ABCD

3. 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

4. 新时期我国商用密码发展的主要任务包括（　）。
A.深化商用密码管理改革

B.强化商用密码专控管理
C.强化商用密码自主创新
D.推进商用密码合规正确有效应用
答案：ACD

5. 某关键信息基础设施运营者未按照要求开展商用密码应用安全性评估，导致因商用密码产品存在安全漏洞而产生大规模的用户数据泄露，根据《中华人民共和国密码法》，针对该行为，下列正确的表述有（　　）。
A、对其进行警告
B、吊销相关资质
C、对关键信息基础设施的运营者处以罚款
D、对直接负责的主管人员处以罚款
答案：CD

6. 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

7. 某涉及国家秘密的科研院所正在建设新的涉密信息系统，需要按照《中华人民共和国密码法》的要求使用密码。以下关于核心密码、普通密码使用要求的说法，正确的有（　）
A、在有线通信中传递的国家秘密信息，应当使用核心密码或普通密码进行加密保护
B、在无线通信中传递的国家秘密信息，应当使用核心密码或普通密码进行加密保护
C、存储国家秘密信息的信息系统，应当使用核心密码或普通密码进行安全认证
D、处理国家秘密信息的信息系统，可以使用商用密码替代核心密码
答案：ABC

8. 某商用密码产品进口企业需要了解商用密码进出口管理的相关规定。根据《中华人民共和国密码法》及配套规定，以下关于商用密码进出口的说法，正确的有（　）
A、商用密码进口许可清单由国务院商务主管部门会同国家密码管理部门和海关总署制定并公布
B、商用密码出口管制清单由国务院商务主管部门会同国家密码管理部门和海关总署制定并公布
C、大众消费类产品所采用的商用密码不实行进口许可和出口管制制度
D、所有商用密码产品均需取得进口许可方可进口
答案：ABC

9. 根据《中华人民共和国密码法》，以下属于核心密码和普通密码工作机构的

密码活动的有（　）。
A.密码科研
B.密码生产、服务
C.密码进出口
D.密码使用、销毁
答案：ABD

10. 根据《中华人民共和国密码法》，关于列入网络关键设备和网络安全专用产品目录的商用密码产品，以下说法正确的是（　）。
A.一般是涉及国家安全、国计民生、社会公共利益和敏感个人信息的产品
B.应由具备资格的机构检测认证合格后方可销售或者提供
C.商用密码服务使用目录产品的，还需要经商用密码服务认证合格
D.《网络关键设备安全通用要求》和《网络关键设备和网络安全专用产品安全认证实施规则》等提供了检测认证的具体要求
答案：BCD

11. 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

12. 根据《中华人民共和国密码法》，密码管理部门的事中事后监管制度包括哪些内容？（　）
A.建立统一的商用密码监督管理信息平台，向社会发布监管信息
B.开展各类日常监管活动
C.开展随机抽查活动
D.将监管信息与社会信用体系相衔接
答案：ABCD

13. 《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 12
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、某科技公司研发了一款用于企业财务数据加密的商用密码软件。该公司负责人认为，商用密码仅指加密技术本身，不包括相关产品和后续服务，因此该公司只需关注技术研发，无需对产品销售后的技术服务承担任何密码管理方面的义务。
答案：错

5、某县政府认为商用密码管理工作属于国家层面的事务，县级政府不需要承担任何商用密码管理职责，因此未在本县设立专门的密码管理机构。
答案：错

6、某企业向国务院商务主管部门申请商用密码进口许可，提交了相关材料。国务院商务主管部门受理后可在第 50 个工作日作出许可决定。
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、某关键信息基础设施运营者正在建设一套新的信息系统，该系统依法需要使用商用密码进行保护。该运营者认为，可以在系统建成后再考虑商用密码保障系统的建设问题。
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、某电子政务电子认证服务机构因自身过错导致电子签名人在政务活动中遭受了损失。该机构认为，由于电子签名人自身也应当对签名安全性负责，因此该机构不承担任何赔偿责任。
答案：错

12、《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

二、网络安全法律法规 50

一、单选题 30
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. 某市网信办在开展网络安全检查时，发现一家网络公司未制定内部安全管理制度。该公司负责人辩称公司规模较小，不需要建立相关制度。根据《中华人民共和国网络安全法》，该公司的辩解是否成立？（　　）
A.成立，小规模企业可以豁免部分义务
B.不成立，所有网络运营者都应履行网络安全保护义务
C.成立，但需要向监管部门备案
D.不成立，只有取得相关许可的企业才需要履行
答案：B

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. 某市电力公司被认定为关键信息基础设施运营者。根据《中华人民共和国网络安全法》，该公司除履行一般网络运营者的安全保护义务外，还应当履行的特殊义务不包括以下哪项（　　）
A、设置专门安全管理机构和安全管理负责人
B.对安全管理负责人和关键岗位人员进行安全背景审查

C.定期对从业人员进行网络安全教育、技术培训和技能考核
D.将核心数据全部公开以供社会监督
答案：D

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. 某网络运营者未按照网络安全等级保护制度的要求采取防范计算机病毒和网络攻击等技术措施，导致其网络系统被黑客入侵，大量用户数据被窃取。根据《中华人民共和国网络安全法》，对该运营者的处罚，以下说法正确的是（　　）
A.只需责令改正，给予警告
B.可以处一万元以上五万元以下罚款
C.处五万元以上五十万元以下罚款，对直接负责的主管人员处一万元以上十万元以下罚款
D.直接吊销营业执照
答案：C

8. 某关键信息基础设施运营者不履行网络安全保护义务，造成大量数据泄露的严重后果。根据《中华人民共和国网络安全法》第六十一条，该运营者可能面临的最高罚款为（　　）
A.五十万元
B.一百万元
C.二百万元
D.一千万元
答案：D

9. 某网络运营者在处理用户个人信息时，不慎将一批用户数据丢失。根据《中华人民共和国网络安全法》，该运营者应当（　　）
A.自行处理，无需告知用户
B.及时告知用户并向有关主管部门报告
C.只需向主管部门报告，无需告知用户
D.只需告知用户，无需向主管部门报告
答案：B

10. 根据《中华人民共和国网络安全法》第四条规定，网络安全工作坚持的方针是（　　）
A.积极防御、依法管理、确保安全、安全可靠
B.积极利用、科学发展、依法管理、确保安全
C.自主可控、安全可靠、统筹规划、依法管理
D.统筹规划、分步实施、确保安全、科学发展
答案：B

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

13. 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

14. 根据《中华人民共和国网络安全法》第十一条规定，建设、运营网络或者通过网络提供服务，应当维护网络数据的（　　）
A.完整性、保密性和可用性
B.完整性、真实性和时效性
C.保密性、真实性和可追溯性
D.可用性、真实性和完整性
答案：A

15. 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

16. 《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

17. 某跨国企业在中国境内设立研发中心，日常开展用户行为数据的收集、存储和分析工作。该企业的数据合规官正在研究《中华人民共和国数据安全法》的适用范围。根据《中华人民共和国数据安全法》的规定，该研发中心在中国境内开展的数据处理活动应当适用本法。该法的立法目的不包括以下哪一项（　　）。
A.规范数据处理活动，保障数据安全
B.促进数据开发利用
C.保护个人、组织的合法权益
D.促进数据的无条件自由流动
答案：D

18. 某科技公司正在制定内部数据安全管理制度。法务人员需要准确理解《中华人民共和国数据安全法》中“数据”“数据处理”“数据安全”三个核心概念。以下关于这三个概念的说法，错误的是（　　）
A.数据是指任何以电子或者其他方式对信息的记录
B.数据处理包括数据的收集、存储、使用、转移、加工、传输、提供等
C.数据处理包括数据的收集、存储、使用、加工、传输、提供、公开等
D.数据安全是指通过采取必要措施，确保数据处于有效保护和合法利用的状态，以及具备保障持续安全状态的能力
答案：B

19. 某市正在推进智慧城市建设，拟开发一款面向全体市民的智能化公共服务APP。根据《中华人民共和国数据安全法》的规定，提供智能化公共服务时，应当充分考虑（　　）的需求，避免对其日常生活造成障碍。
A.妇女和儿童
B.老年人和残疾人
C.欠发达地区群众
D.外来务工人员
答案：　B

20. 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

21. 某国家机关不履行《中华人民共和国数据安全法》规定的数据安全保护义务，造成政务数据泄露。根据《中华人民共和国数据安全法》的规定，对该国家机关直接负责的主管人员和其他直接责任人员应当（　　）
A.处五万元以上二十万元以下罚款
B.依法给予处分
C.处十日以上十五日以下拘留
D.如认错态度良好则免予处罚
答案： B

22. 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

23. 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

24. 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

25. 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

26. 《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

27. 《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

28. 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

29. 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

30. 根据《电子签名法》的规定，可靠的电子签名与手写签名或者盖章具有什么关系（　）
A. 可靠的电子签名法律效力低于手写签名
B. 可靠的电子签名法律效力高于手写签名
C. 可靠的电子签名与手写签名或者盖章具有同等的法律效力
D. 可靠的电子签名仅在某些特定领域具有法律效力
答案：C

二、多选题 10

1.某市政府在制定本市网络安全工作规划时，需要明确网络安全工作的根本原则。根据《中华人民共和国网络安全法》，网络安全工作应当坚持（　）
A.中国共产党的领导
B.贯彻总体国家安全观
C.以经济效益为中心
D.推进网络强国建设
答案：ABD

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. 国家在推进网络安全工作中，确立了网络安全与信息化发展的关系。根据《中华人民共和国网络安全法》，以下关于这一关系的表述正确的有（ ）。
A.国家坚持网络安全与信息化发展并重
B.遵循积极利用、科学发展、依法管理、确保安全的方针
C.应当优先保障网络安全，暂缓信息化发展
D.国家鼓励网络技术创新和应用，支持培养网络安全人才
答案：ABD

4. 甲公司拟与乙公司签订一份货物买卖合同，双方通过电子邮件协商一致后，甲公司使用其法定代表人王某的数字证书对合同电子版进行了电子签名。根据《中华人民共和国电子签名法》，下列有关电子签名的表述中，正确的有（ ）。
A.电子签名是指数据电文中以电子形式所含、所附用于识别签名人身份并表明签名人认可其中内容的数据
B.电子签名必须采用数字证书的形式才具有法律效力
C.电子签名具有识别签名人身份和表明签名人认可文件内容的双重功能
D.电子签名必须以磁介质为载体生成
答案：AC

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. 某市供水公司拟通过电子方式与用户签订供水服务合同，用户张某对该合同的电子形式提出异议。根据《中华人民共和国电子签名法》，下列表述正确的有（ ）。
A.涉及停止供水等公用事业服务的文书不适用电子签名
B.供水服务合同可以采用电子方式签署
C.涉及停止供电的文书不适用电子签名
D.所有公用事业服务合同均不得采用电子方式签署
答案：AC

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. 小李在某购物平台注册时同意平台收集其浏览记录和购物偏好用于个性化推荐。使用一段时间后，小李认为推荐不准确，决定撤回同意。平台告知小李：撤回同意后，之前基于同意已进行的推荐活动无效，且以后不再向其提供任何服务。关于平台的说法，下列评价正确的有（　）。
A.平台应提供便捷的撤回同意方式
B.撤回同意不影响撤回前已进行的个人信息处理活动的效力
C.平台可以因小李撤回同意而拒绝继续提供服务
D.平台不得以撤回同意为由拒绝提供产品或者服务，但处理个人信息属于提供服务所必需的除外
答案：ABD

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. 某公司法定代表人王某的电子签名制作数据（私钥）存储在公司的服务器中，公司 IT 部门主管张某未经王某授权，使用该私钥签署了一份借款合同。根据《中华人民共和国电子签名法》，该数据电文应视为王某发送。
答案：错

5. 某在线教育平台在课程结束后，仍继续保存所有学员的姓名、联系方式、学习记录等全部个人信息。平台认为只要学员没有主动要求删除，就可以一直保存。
答案：错

6. 某境外电子认证服务提供者在境外签发的电子签名认证证书，经国务院信息产业主管部门核准后，与依照《中华人民共和国电子签名法》设立的境内电子认证服务提供者签发的证书具有同等的法律效力。
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. 网络运营者为用户办理网络接入、域名注册服务时，应当要求用户提供真实身份信息；用户不提供真实身份信息的，网络运营者可以酌情为其提供有限服务。
答案：错

10. 《中华人民共和国数据安全法》规定从事数据交易中介服务的机构提供服务，应当要求数据提供方说明数据来源，审核交易双方的身份，并留存审核、交易记录。
答案：对

三、密码管理规章制度 55

一、单选题 35
1. 依据《电子印章管理办法》，电子印章的法律效力如何规定？（ ）
A. 与实物印章效力相同
B. 效力低于实物印章
C. 仅在政务活动中有效

D. 需另行公证方有效
答案：A

2. 依据《电子印章管理办法》，电子印章有效期截止时间不得晚于（ ）。
A. 实物印章有效期
B. 电子印章所有者电子签名认证证书有效期的截止时间
C. 电子印章制作管理单位规定的统一日期
D. 电子印章备案时间后一年
答案：B

3. 依据《电子印章管理办法》，电子印章的本质是什么？（ ）
A. 实物印章的数字化图片
B. 基于密码技术和相关数字技术表征印章的特定格式数据
C. 单位内部使用的电子签名工具
D. 用于替代手写签名的图像文件
答案：B

4. 依据《电子印章管理办法》，电子印章使用管理应遵循的原则是（ ）。
A. 谁制作、谁负责
B. 谁持有、谁使用
C. 谁所有、谁控制，谁签章、谁负责
D. 谁备案、谁管理
答案：C

5. 依据《电子印章管理办法》，电子印章管理工作应遵循的原则不包括以下哪项？（ ）
A. 统筹推进
B. 分级管理
C. 自主自愿
D. 安全可控
答案：C

6. 依据《电子印章管理办法》，负责电子印章相关电子政务电子认证服务监督管理的是（ ）
A. 国务院办公厅
B. 工业和信息化部
C. 国家密码管理局
D. 公安机关
答案：C

7. 依据《电子印章管理办法》，电子印章的电子签名认证证书应由（ ）签发。
A. 任意电子认证服务机构
B. 依法设立的电子政务电子认证服务机构或电子认证服务机构
C. 电子印章制作管理单位自行签发
D. 公安机关

答案：B

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. 电子印章所有者在哪种情况下应当注销电子印章？（ ）
A. 电子印章载体损坏
B. 电子印章有效期到期
C. 单位更名、解散、撤销、被吊销等情形
D. 电子印章图像样式调整
答案：C

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. 依据《电子印章管理办法》，负责依法打击涉及电子印章违法犯罪行为的部门是（ ）。
A. 国家密码管理局
B. 工业和信息化部
C. 公安机关
D. 国务院办公厅
答案：C

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，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

24. 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

25. 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

26. 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

27. 《电子印章管理办法》正式实施日期为（　　）。
A. 2025 年 9 月 27 日
B. 2025 年 10 月 1 日
C. 2026 年 1 月 1 日
D. 印发之日起
答案：D

28. 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

29. 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

30. 根据《电子印章管理办法》，某单位（组织）申请制作电子印章时，应当提交的材料中不包括以下哪项？（　　）
A. 电子印章申请通过的相关证明材料
B. 单位（组织）的设立批准文件或者设立登记证件
C. 制作电子印章的相关数据和信息
D. 电子印章所有者的电子签名认证证书
答案：D

31. 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

32. 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

33. 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

34. 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

35. 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

二、多选题 10
1.　以下哪些属于网络数据处理者在按照有关部门要求委托评估机构开展风险评估时应履行的义务？（　　）
A. 为评估机构提供必要的访问权限支持
B. 在限定时间内完成风险评估

C. 在完成评估后将风险评估报告报送有关部门
D. 对风险评估中发现的问题进行整改并报送整改情况
答案：ABCD

2. 《网络数据安全风险评估办法》规定，省级以上网信部门、电信主管部门、公安机关和其他有关部门在哪些情形下可以要求网络数据处理者委托通过认证的评估机构开展风险评估？（ ）
A. 网络数据处理活动存在较大安全风险，可能危害国家安全、公共利益的
B. 发生网络数据安全事件，导致重要数据或者大规模个人信息泄露、被窃取的
C. 网络数据处理者认为自身风险较高的
D. 有关部门规定的其他情形
答案：ABD

3. 根据《网络数据安全风险评估办法》，评估机构开展网络数据安全风险评估时应当遵守哪些基本要求？（ ）
A. 遵守法律法规
B. 公正客观地作出风险判断
C. 对所出具的风险评估报告真实性、有效性、完整性负责
D. 根据网络数据处理者的要求灵活调整评估结论
答案：ABC

4. 以下关于网络数据安全风险评估报告编制与保存的说法，正确的有：
A. 重要数据处理者编制的风险评估报告至少保存 3 年
B. 一般数据处理者可以参照国家标准编制风险评估报告
C. 重要数据处理者应当严格按照国家标准编制风险评估报告，不得参照行业规定
D. 风险评估报告需由评估机构主要负责人和评估负责人签字并加盖公章
答案：ABD

5. 依据《网络数据安全风险评估办法》，以下哪些属于国家相关部门在风险评估工作中的职责？
A. 国家网信部门会同国务院电信、公安等有关部门建立专项工作机制
B. 国家网信部门汇总风险评估报告并与国务院电信、公安、国家安全等有关部门共享
C. 有关主管部门应于每年 1 月底前将年度风险评估检查计划报送国家网信部门
D. 省级以上网信部门可以对重要数据处理者的风险评估报告进行检查核验
答案：ABCD

6. 下列哪些部门（或单位）对电子印章负有监督管理职责？（ ）
A. 国家密码管理局
B. 工业和信息化部
C. 公安机关
D. 国务院办公厅
答案：ABCD

7. 电子印章制作应当符合哪些要求？（ ）

A. 电子签名认证证书合法有效
B. 数据格式、生成流程和应用接口符合国家有关标准规范
C. 图像规格式样与实物印章完全一致，不可附加标注
D. 图像规格、式样应与印章管理有关法律法规明确的印模规制保持一致
答案：ABD

8. 电子印章状态信息备案的情形包括哪些？（ ）
A. 电子印章制作完成
B. 电子印章停用
C. 电子印章恢复
D. 电子印章图像样式变更
答案：ABC

9. 依据《电子印章管理办法》，一个完整的电子印章包含哪些内容？（ ）
A. 印章图像数据
B. 印章名称
C. 印章所有者信息
D. 电子签名认证证书
答案：ABCD

10. 依据《电子印章管理办法》，下列哪些行为依法依规应承担相应责任？（ ）
A. 伪造电子印章
B. 变造电子印章
C. 冒用电子印章
D. 盗用电子印章
答案：ABCD

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. 处理一般数据的网络数据处理者应当至少每 2 年开展一次风险评估。（ ）
答案：错

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. 评估机构在风险评估过程中发现重大数据安全风险时，应当首先向有关主管部门报告，再通知网络数据处理者。（ ）
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. 有关主管部门开展数据安全检查时，不得向被检查的重要数据处理者收取任何费用。（　　）
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. 评估机构接受数据安全风险评估委托后，可以根据需要将部分评估工作转委托给其他专业机构完成。（　　）
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. 对同一网络数据安全事件或者风险，有关部门可以要求多个评估机构同时对该网络数据处理者开展风险评估，以确保评估结论的准确性。（　）
答案：错

四、其他政策法规条例 45

一、单选题 25

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. 根据《电子认证服务使用密码管理办法》，申请《电子认证服务使用密码许可证》的机构，应当向哪个部门提交申请材料？（ ）
A. 国家密码管理局
B. 国家密码管理局委托进行受理的省、自治区、直辖市密码管理部门
C. 国务院工业和信息化主管部门
D. 住所地的县级以上地方各级密码管理部门
答案：B

7. 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

8. 根据《网络数据安全风险评估办法》，重要数据处理者应当多久开展一次年度风险评估？
A. 每半年
B. 每年度
C. 每 2 年
D. 每 3 年

答案：B

9. 重要数据处理者在完成年度风险评估后，应当在多少个工作日内向有关主管部门报送风险评估报告？
A. 10 个工作日
B. 15 个工作日
C. 20 个工作日
D. 30 个工作日
答案：C

10. 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

11. 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

12. 获得《电子认证服务使用密码许可证》的机构，其机构名称发生变更的，应当自变更之日起多少日内向国家密码管理局办理变更手续？（ ）
A. 15 日
B. 20 日
C. 30 日
D. 60 日
答案：C

13. 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

14. 依据《网络数据安全风险评估办法》，评估机构及其关联机构不得连续多少次以上对同一网络数据处理者开展年度风险评估？
A. 2 次

B. 3 次
C. 4 次
D. 5 次
答案：B

15. 获得《电子认证服务使用密码许可证》的机构，应当自行或者委托专业机构每年至少进行（　　）次电子认证服务使用密码合规性评估？
A. 1
B. 2
C. 3
D. 4
答案：A

16. 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

17. 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

18. 络数据处理者按照有关部门要求委托评估机构开展风险评估，在整改完成后，应在多少天内向有关部门报送整改情况报告？
A. 10 个工作日
B. 15 个工作日
C. 20 个工作日
D. 30 个工作日
答案：B

19. 《网络数据安全风险评估办法》自（　　）起开始施行？
A. 2026 年 6 月 18 日
B. 2026 年 6 月 1 日
C. 2026 年 8 月 20 日
D. 2026 年 1 月 1 日
答案：C

20. 《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

21. 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

22. 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

23. 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

24. 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

25. 《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

二、多选题 10
1. 依据《网络数据安全风险评估办法》，有关主管部门应当按照（　　）原则组织开展本行业、本领域的风险评估工作。
A. 谁管业务
B. 谁管业务数据
C. 谁管数据安全
D. 谁管网络安全
答案：ABC

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
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. 根据《电子认证服务使用密码管理办法》，申请《电子认证服务使用密码许可证》应当具备的条件包括（ ）。
A. 具有企业法人资格
B. 具有在境内设置、符合国家有关密码标准的电子认证服务系统
C. 具有密码或者相关专业知识的专业人员
D. 注册资本不低于 5000 万元
答案：ABC

4. 有下列情形之一的，获得《电子认证服务使用密码许可证》的机构应当向国家密码管理局办理变更手续（ ）。
A. 机构法定代表人发生变更
B. 机构注册地址发生变更
C. 电子认证服务系统进行搬迁
D. 机构年度财务审计报告出具
答案：ABC

5. 国家密码管理局在对行政许可申请进行审查时，可以采取的技术评审方式包括（ ）。
A. 电子认证服务系统安全性审查
B. 互联互通测试
C. 运营场所、设备设施实地查勘
D. 管理体系实地查勘
答案：ABCD

6. 密码管理部门在监督检查中，应遵守的义务包括（ ）。
A. 不得影响电子认证服务系统的正常运行
B. 不得收取任何费用
C. 不得泄露在履行职责中知悉的商业秘密
D. 检查人员不得少于三人
答案：ABC

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. 获得《电子认证服务使用密码许可证》的机构违反《电子认证服务使用密码管理办法》相关规定，可能面临的行政处罚包括（ ）。
A. 警告
B. 通报批评
C. 罚款
D. 吊销营业执照
答案：ABC

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. 依据《网络数据安全风险评估办法》，风险评估包括哪些活动？（　　）
A. 风险识别
B. 风险分析
C. 风险评价
D. 风险处置
答案：ABC

三、判断题 10
1. 《电子认证服务使用密码管理办法》的施行日期是 2026 年 7 月 1 日，同时废止了 2009 年发布的旧版办法。
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. 获得《电子认证服务使用密码许可证》的机构，其相关专业技术人员和安全管理人员每年的密码安全教育培训时间不得少于 20 个小时。
答案：对

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. 因许可证有效期满需要延续的，机构应当在有效期届满 30 日前向国家密码管理局提出书面申请。
答案：错

7. 电子认证服务系统所需的密钥服务，可以由机构自行搭建的密钥管理系统提供。
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. 如果《电子认证服务使用密码许可证》被依法吊销，国家密码管理局应当将有关情况通报国务院工业和信息化主管部门。
答案：对

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 835

一、密码学 395

一、单选题 155

1. 以下哪种情况可以实现对消息完整性的认证，也提供消息源真实性鉴别（　）。

A.对消息进行 SM3 杂凑计算，将消息和杂凑值一并发送给接收者

B.对消息进行 SM4-CTR 计算，将密文发送给接收者

C.对消息进行 SM2 签名计算，将消息和签名一并发送给接收者

D.对消息进行 SM3 杂凑计算，将消息发送给接收者，并通过可靠的方式将消息的摘要离线发送给接收者，保证摘要值无法被攻击者篡改

答案：C

2. 打扑克是一种流行于全世界的休闲类游戏，玩扑克之前首先要进行洗牌，从密码学的角度看，可以将洗牌理解为一种加密运算，目的是让玩家猜不到牌的顺序，那么这种加密运算属于（　）。

A、置换加密

B、代换加密

C、公钥加密

D、序列加密

答案：A

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. 在下面分组密码加密工作模式中，有密文传输错误扩散的是（　）。

A.ECB

B.OFB

C.CBC

D.CTR

答案：D

5. 在量子攻击下，根据 Grover 算法，采用 SM4 的分组密码 CTR 模式抵抗密钥恢复攻击的强度大约是（　）。

A.2^32

B.2^64

C.2^96

D.2^128

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. DES 算法中扩展运算 E 的功能是（　　）。
A.对 16 位的数据组的各位进行选择和排列，产生一个 32 位的结果
B.对 32 位的数据组的各位进行选择和排列，产生一个 48 位的结果
C.对 48 位的数据组的各位进行选择和排列，产生一个 64 位的结果
D.对 56 位的数据组的各位进行选择和排列，产生一个 64 位的结果
答案：B

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. 如果 DES 加密使用的轮密钥为 k1，k2……k16，则 DES 解密时第一轮使用的密钥为（　　）。
A.K1
B.K8
C.K12
D.K16
答案：D

10. 下面关于 AES 算法的叙述，哪一个是正确的？（　　）
A.AES 算法是用 56 比特的密钥加密 64 比特的明文得到 64 比特的密文
B.AES 算法属于非对称密码算法
C.AES 是一个数据块长度和密钥长度可分别为 128 比特、192 比特或 256 比特的分组密码算法
D.AES 是一个数据块长度和密钥长度可分别为 64 比特或 128 比特的分组密码算法
答案：C

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. 某业务员发起了“从 A 账户向 B 账户转账 1 亿元”的转账请求数据并进行加密传输，攻击者将捕获的密文分组数据进行对调，将原转账请求内容改为“从 B 账户向 A 账户转账 1 亿元”，以下加密模式可能会导致该问题发生的是（　　）。
A.CBC
B.ECB
C.BCC
D.CFB
答案：B

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. SM4 算法的密钥和明文长度分别是多少比特？（　　）。
A.128、256
B.128、128
C.256、128
D.256、256
答案：B

18. AES 算法中的状态可表示为一个二维数组，如果明文长度为 128 比特，则明文状态为（　　）。

A.4 行 4 列
B.4 行 6 列
C.4 行 8 列
D.4 行 10 列
答案：A

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 算法是我国国家密码管理局发布的商用密码标准，其广泛应用于金融数据传输、电子商务安全、电子政务等场景。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. 我国商用分组密码算法 SM4 加密的轮数为（　　）。
A.12 轮
B.14 轮
C.16 轮
D.32 轮
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. 下列分组密码认证模式中，使用密钥最少的是（　　）。
A.OMAC
B.TMAC
C.XCBC
D.EMAC
答案：A

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. 如果泄漏了 CBC-MAC 的链接值，会导致如下情况发生（　　）。
A.密钥被恢复
B.CBC-MAC 被伪造
C.生成标签错误
D.无任何问题
答案：B

31. 关于 DES 加密算法和 AES 加密算法的说法中错误的是（　　）。
A.DES 是一个分组算法，数据分组长度为 64 比特位
B.AES 是一个分组密码算法，数据分组长度为 128 比特位
C.DES 和 AES 均为对称密钥加密算法
D.DES 和 AES 密钥长度为 128 比特位（16 字节）
答案：D

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. 消息鉴别码比杂凑函数增加了（　　）功能。
A.机密性保护
B.完整性保护
C.消息源鉴别
D.不可否认性
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. SM4 加密轮函数中的线性变换由输入及其循环左移若干比特共（　　）项异或而成。
A.4
B.5
C.8
D.32
答案：B

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. 为确保加解密结构一致，SM4 算法最后还需经过一次（　）运算。
A.反序变换
B.交叉变换
C.非线性变换
D.正形置换
答案：A

40. DES 算法密钥是 64 位，其中密钥有效位为（　）。
A.32 比特
B.56 比特
C.64 比特
D.128 比特
答案：B

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. DES 中密钥从输入的 64 位到输入 F 函数中，轮密钥长度为（　　）。
A.64 比特
B.48 比特
C.128 比特
D.36 比特
答案：B

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. 相比于 RSA 算法，SM2 算法在相同安全强度下，所需的密钥长度要短得多，因此 SM2 算法适合在移动设备、智能卡等资源受限的环境中使用。那么，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. SM4 密钥扩展算法中首先将加密密钥与（　　）异或。

A.系统参数
B.固定参数
C.轮常数
D.明文
答案：A

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. 如果 M，C，K 分别表示明文、密文和密钥，而 M'，C'，K'分别表示的非，E 表示加密运算，则 DES 算法的互补对称性可以表示为（　）。
A、C＝E（M，K），则 C'＝E（M'，K'）
B、C＝E（M，K），则 C'＝E（M，K）
C、C＝E（M，K），则 C'＝E（M，K'）
D、C＝E（M，K），则 C'＝E（M'，K）
答案：A

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. OFB 是一种分组密码（　）模式。
A.加密
B.认证
C.认证加密
D.杂凑
答案：A

56. SM4 是我国提出的商用密码算法，SM4 算法进行加解密时的迭代次数是（　）。
A.10

B.16
C.31
D.32
答案：D

57. CCM 是 CTR 工作模式和 CBC-MAC 消息鉴别码以（　　）的形式进行结合。
A.MAC-then-Encrypt
B.Encrypt-then-MAC
C.Encrypt-and-MAC
D.Hash-then-Encrypt
答案：A

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. Skipjack 是一个密钥长度为（　　）位分组加密算法。
A.56
B.64
C.80
D.128
答案：C

下列分组密码工作模式，在解密过程中具备错误传播扩散的是（　　）。
A.ECB
B.OFB
C.CFB
D.CTR
答案：C

60. 当 SM4 算法采用（　　）工作模式时，可以并行处理多组消息分组。
A.ECB
B.CBC
C.CFB
D.OFB
答案：A

61. ZUC 算法比特重组 BR 层从上层 LFSR 寄存器单元抽取位置不包括（　　）。
A.s0
B.s5
C.s9
D.s12

答案：D

62. ZUC-128 主算法一次输出的密钥流长度为（　　）。
A.32 比特
B.64 比特
C.128 比特
D.256 比特
答案：A

63. 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

64. ZUC 算法非线性函数 F 部分包含 2 个（　　）比特的记忆单元。
A.8
B.16
C.32
D.64
答案：C

65. 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

66. ZUC 算法驱动部分 LFSR 的反馈抽头位置不包括（　　）。
A.S15
B.S10
C.S7
D.S0
答案：C

67. 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

68. ZUC 算法的非线性函数 F 的设计采用了 4 个（　　）比特的 S 盒。
A.4×4

B.8×8
C.16×16
D.32×32
答案：B

69. 在 AES-128 加密过程中，需要生成 11 个轮密钥（初始轮密钥+10 轮）。下列关于 AES 密钥扩展的描述，错误的是（　　）。
A.当轮数不为 4 的倍数时，密钥扩展直接使用异或操作
B.当轮数为 4 的倍数时，需要使用 S 盒进行字节替换
C.AES-192 的轮密钥扩展与 AES-128 完全相同
D.轮密钥扩展引入了非线性变换以抵抗密码分析
答案：C

70. 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

71. 关于国密算法 SM1 和 SM4 的描述，正确的是（　　）。
A.SM1 和 SM4 都是公开算法，都可以在软件中自由实现
B.SM1 是硬件实现的对称密码算法，不公开算法细节；SM4 是公开的分组密码算法
C.SM1 和 SM4 都是非对称密码算法
D.SM1 的分组长度为 64 位，SM4 的分组长度为 128 位
答案：B

72. 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

73. 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

74. 某公司仍在使用 DES 算法加密历史数据。已知 DES 的有效密钥长度为 56 位，在当今计算能力下，以下（　　）项攻击方式对 DES 最具威胁。
A.差分密码分析
B.线性密码分析

C.暴力破解攻击
D.侧信道攻击
答案：B

75. 某物联网设备需要传输不定长的传感器数据，且要求每个数据包独立解密（允许数据包丢失不影响其他包），同时不希望密文长度明显增加。以下（　　）种工作模式最合适。
A.ECB 模式
B.CBC 模式
C.CFB 模式
D.CTR 模式
答案：D

76. （　　）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

77. 3DES（三重 DES）采用 EDE 模式（加密-解密-加密）使用两个或三个密钥。以下关于 3DES 的说法，错误的是（　　）。
A.使用两个密钥的 3DES 有效密钥长度为 112 位
B.3DES 的加密速度比 AES 慢
C.3DES 仍然被认为是安全的，可以用于新系统设计
D.3DES 的中间相遇攻击复杂度为 O(2^56)
答案：C

78. 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

79. SM4 的密钥扩展算法将 128 位初始密钥扩展为 32 个轮密钥。关于 SM4 密钥扩展的描述，正确的是（　　）
A.密钥扩展算法与加密算法完全不同，没有共同点
B.密钥扩展算法使用了与加密算法相同的 S 盒和线性变换
C.密钥扩展算法不需要 S 盒，仅使用线性变换
D.密钥扩展算法的轮数与加密算法不同
答案：B

80. 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

81. 在使用 AES-CBC 模式加密数据时，需要对明文进行填充。以下关于 PKCS#7 填充的描述，正确的是（　　）。
A.如果明文长度恰好是分组长度的整数倍，则不需要填充
B.填充的每个字节的值等于需要填充的字节数
C.填充的最后一个字节固定为 0x80
D.填充长度最小为 0 字节，最大为 15 字节
答案：B

82. 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

83. SM3 算法的消息摘要长度为 256 位，其输入消息的最大长度限制是（　　）。
A.2^64 - 1 位
B.2^64 - 1 字节
C.无限制
D.2^128 - 1 位
答案：A

84. 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

85. 某遗留系统仍在使用 MD5 进行文件完整性校验。关于 MD5 算法的安全性，以下说法正确的是（　　）。
A.MD5 的输出长度为 160 位，抗碰撞强度为 80 位
B.MD5 已经可以产生碰撞，但无法产生原像攻击，因此仍可用于数字签名
C.MD5 已被证明存在碰撞攻击，不应再用于安全性要求高的场合
D.MD5 的抗碰撞强度为 2^128，仍然足够安全
答案：C

86. 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

87. 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

88. 关于 SHA-256 和 SM3 的对比，以下描述正确的是（　　）。
A.SHA-256 和 SM3 的压缩函数结构完全相同
B.SHA-256 采用 64 轮迭代，SM3 采用 64 轮迭代
C.SM3 的设计借鉴了 SHA-256 但加入了独特的消息扩展和压缩函数设计
D.SHA-256 比 SM3 更安全，因为 SHA-256 的摘要更长
答案：C

89. 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

90. 某 Web 系统使用哈希加盐的方式存储用户密码。关于盐值的说法，以下错误的是（　　）。
A.盐值应随机生成，每个用户使用不同的盐值
B.盐值可以与密码哈希值一起存储
C.盐值的作用是抵抗彩虹表攻击
D.盐值需要保密，不能与哈希值一起存储
答案：D

91. SM3 算法的消息填充规则是：先填充"1"，后填充"0"，直到消息长度对 512 取模等于 448，最后填充 64 位的原始消息长度。如果原始消息长度为 448 位（恰好等于填充条件值），则需要填充（　　）位。
A.0 位（不需要填充）
B.1 位
C.512 位（完整的一个分组）
D.64 位
答案：C

92. 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

93. 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

94. 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

95. 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

96. 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

97. SM2 是我国自主设计的椭圆曲线公钥密码算法。关于 SM2 的描述，以下错误的是（　　）。
A.SM2 基于椭圆曲线离散对数问题（ECDLP）的困难性
B.SM2 可以用于数字签名、密钥交换和公钥加密
C.SM2 的推荐椭圆曲线参数使用 256 位素数域曲线
D.SM2 的密钥长度与 RSA-2048 相同，安全性也相同
答案：D

98. 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

99. SM9 是我国自主设计的基于标识的密码算法（Identity-Based Cryptography, IBC）。关于 SM9 的特点，以下描述正确的是（　　）。
A.SM9 不需要证书管理机构（CA），但需要一个密钥生成中心（KGC）
B.SM9 的用户公钥是随机生成的，与用户身份无关
C.SM9 与 SM2 的安全性假设完全相同
D.SM9 不支持加密和签名，仅支持密钥交换
答案：A

100. 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

101. 以下关于 SM2 数字签名、RSA 数字签名和 ECDSA 的对比，描述正确的是（　　）。
A.三种签名算法的签名长度相同
B.SM2 和 ECDSA 都可以实现签名聚合，RSA 不支持
C.SM2 签名算法中包含一个额外的哈希函数调用，而 ECDSA 不包含
D.SM2 的签名验证过程中不需要计算哈希值
答案：B

102. 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

103. 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
104. 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

105. 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

106. 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

107. 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

108. 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

109. 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

110. 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

111. 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

112. 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

113. 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

114. 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

115. 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

116. 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

117. 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

118. 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

119. 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

120. 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

121. 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

122. 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

123. 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

124. 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

125. 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

126. 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

127. 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

128. 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

129. 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

130. 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

131. 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

132. 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

133. 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

134. 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

135. 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

136. 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

137. 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

138. （ ）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

139. 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

140. 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

141. 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

142. 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

143. 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

144. 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

145. 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

146. 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

147. 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

148. 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

149. Alice 破解了某系统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

150. 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

151. SM2 密钥交换协议（基于 ECDH）可以使得通信双方在公开信道上协商出共享秘密。以下关于 SM2 密钥交换的描述，错误的是（　）
A. SM2 密钥交换使用椭圆曲线点乘运算
B. 通信双方各自生成临时密钥对，并交换临时公钥
C. SM2 密钥交换最终协商出的共享密钥可以直接用作对称加密密钥
D. SM2 密钥交换协议通过哈希运算对交换过程进行认证，防止中间人攻击
答案：C

152. 前向安全性（Forward Secrecy）是指长期私钥泄露后，过去的会话密钥仍然安全。以下密钥交换方案中，提供完美前向安全性的是（　）
A. RSA 密钥传输（客户端生成预主密钥，用 RSA 公钥加密后发送给服务器）
B. 静态 ECDH（双方使用固定长期的椭圆曲线密钥对）
C. ECDHE（临时椭圆曲线 Diffie-Hellman 密钥交换）
D. SM2 密钥封装机制（KEM）
答案：C

153. 量子计算机对当前主流的公钥密码算法构成威胁。以下算法中，受量子计算机影响最大的是（　）
A. AES-256
B. SM3
C. SM2
D. SM4
答案：C

154. 某数据库系统需要对存储的每条记录进行加密，并且需要能够检测数据是否被篡改。以下方案中最优的是（　）
A. AES-CBC 加密 + 独立存储哈希值
B. AES-GCM 认证加密
C. 先 AES-ECB 加密，再计算 MD5
D. 仅使用 SM3 进行完整性保护，不加密
答案：B

155. 差分密码分析是一种针对分组密码的选择明文攻击方法。以下关于差分密码分析的描述，正确的是（　　）
A. 差分密码分析通过分析大量明密文对的线性关系来恢复密钥
B. 差分密码分析的核心是研究输入差分对输出差分的影响规律
C. 差分密码分析对 DES 完全无效
D. 差分密码分析是唯密文攻击方法
答案：B

二、多选题 130
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. 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

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. 一个完整的密码体制，包括以下（　　）要素。
A.明文空间
B.密文空间
C.数字签名
D.密钥空间
答案：ABD

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. 下列可以防止重放攻击的方式有（　）。
A.时间戳
B.鉴别方验证序列号没有重复
C.采用“挑战-响应”机制
D.数字签名
答案：ABC

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. 对 DES 的三种主要攻击方法包括（　）。
A.暴力攻击
B.生日攻击
C.差分密码分析
D.线性密码分析
答案：ACD

9. 以下加密算法中不属于古典加密算法的是（　）。
A.Caesar 密码
B.DES 算法
C.IDEA 算法
D.Diffie-Hellman 算法
答案：BCD

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 Integer Solution）
答案：ABCD

11. 一个密码系统的安全性包含哪些？（　）
A.加密安全性
B.解密安全性
C.可证明安全性
D.计算安全性
答案：CD

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

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，很难找到一个特定输入 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. 以下关于密钥的描述，正确的是（　）。
A.在消息认证码中，发送者和接收者使用共享的密钥来进行认证
B.在数字签名中，签名的生成和验证使用不同的密钥
C.消息认证码所使用的密钥，是用于认证的密钥
D.对称密码和非对称加密的密钥都可以用于机密性保护
答案：ABCD

20. 在计算复杂性理论中，下列属于 NP 问题的是（　）。
A、背包问题
B、整数分解问题
C.矩阵覆盖问题
D.陪集重量问题
答案：ABCD

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. 一个有新鲜性的值是指这个值是刚产生的，而不是重放的。常用的保证新鲜性的机制有（　）。
A.时间戳
B.一次性随机数
C.计数器
D.将时间戳和计数器结合使用的方法
答案：ABCD

25. 下列方法可用于对消息认证码攻击的是（　）。
A.重放攻击
B.密钥推测攻击
C.已知明文攻击
D.选择密文攻击
答案：AB

26. 公钥密码体制使用不同的加密密钥和解密密钥。以下密码算法是公钥密码体制的有（　）。
A.SM2
B.SM4
C.Rabin
D.RSA
答案：ACD

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. 下列攻击形式中，属于主动攻击的是（　　）。
A.伪造
B.篡改
C.中断
D.监听
答案：ABC

33. 下列密码分析方法属于已知明文攻击的是（　　）。
A.最佳放射逼近分析方法
B.线性密码分析方法
C.分别征服分析方法
D.时间-存储权衡攻击
答案：AB

34. 下列分组密码工作模式中，加密不能并行但解密可并行的是（　　）。
A.CBC
B.OFB
C.CFB
D.CTR
答案：AC

35. 下述正确描述 SM4 和 AES 有什么不同之处的是（　　）。
A.SM4 密钥长度固定，而 AES 密钥长度可变
B.SM4 的线性变换是面向比特的运算，而 AES 的所有运算是面向字节的
C.SM4 的加密过程和解密过程一致，而 AES 的加密过程和解密过程不一致
D.SM4 是非平衡广义 Fesitel 结构，而 AES 是 SP 结构
答案：ABCD

36. 对称密码的优点是非常快速，受到广泛的应用，选项中哪些是对称密码算法？（　　）
A.RSA 算法

B.3DES 算法
C.SM4 算法
D.IDEA 算法
答案：BCD

37. 对于 SM4 分组密码，当采用 CTR 工作模式时，下述描述正确的是（　）。
A.具有良好的硬件和软件效率
B.能进行随机访问
C.可以在明文到来之前计算密钥流
D.不能用于高速实现需求
答案：ABC

38. 以下分组密码算法的工作模式 IV 要求每个消息必须唯一，不能重用，且不可预测的是（　）。
A.OFB
B.CFB
C.CBC
D.GCM
答案：ABCD

39. 主动攻击者可以通过将事先保存的正确 MAC 值不断重放来发动攻击。以下哪几种方法可以防御重放攻击？（　）
A.每次都对发送的消息赋予一个递增的编号（序号），并且在计算 MAC 值时将序号也包含在消息中
B.在发送消息时包含当前的时间，如果收到以前的消息，即便 MAC 值正确也将其当做错误的消息来处理
C.在通信之前，接收者先向发送者发送一个一次性的随机数，发送者在消息中包含这个 nonce 并计算 MAC 值
D.每次都对发送的消息携带发送者的唯一身份标识，并且在计算 MAC 值时该标识也包含在消息中
答案：ABC

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. SM4 分组密码算法可以用于下列哪些用途？（　）
A.数据保密传输
B.信息加密存储
C.签名认证
D.消息鉴别码
答案：ABD

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. 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

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. 不借助其他密码机制，分组密码算法自身可实现（　　）。
A.加密功能
B.认证功能
C.数据完整性保护功能
D.数字签名功能
答案：ABC

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. 下列分组密码工作模式中，解密之前可以进行伪随机流预计算的有（　　）。
A.CBC
B.CTR

C.OFB
D.CFB
答案：BC

49. Shannon 建议密码设计的基本方法包括（　　）。
A.布尔运算
B.扩散
C.混淆
D.迭代
答案：BC

50. 以下分组密码算法工作模式，说法是正确的（　　）。
A.在 CRT 模式中，主动攻击者可以通过反转密文分组中的某些比特，引起解密后明文中的相应比特也发生反转
B.在 OFB 模式中，可以在加密消息之前预计算密钥流
C.CFB 模式与 OFB 模式的区别仅仅在于密码算法的输入
D.假设 CBC 模式加密的密文分组中有一个分组损坏了（如由于硬盘故障导致密文分组的值发生了改变），在这种情况下，只要密文分组的长度没有发生变化，则解密时最多只会有 2 个分组受到数据损坏的影响
答案：ABCD

51. SM4 分组密码算法轮函数中的 T 置换，包括的运算有（　　）。
A.非线性变换
B.S 盒运算
C.线性变换
D.列混合变换
答案：ABC

52. 下述对 SM4 分组密码算法介绍中正确的是（　）。
A.将消息分为固定长度的数据块来逐块处理的
B.分组长度和密钥长度一样长
C.分组长度和密钥长度不一样
D.加密算法中的线性变换与密钥扩展算法中的线性变换完全一致
答案：AB

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. 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

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. 分组密码将明文消息编码表示后的数字序列进行分组划分并进行加密，下列不属于分组密码体制的有（　）。
A.SM2 密码体制
B.IDEA 密码体制
C.RC5 密码体制
D.ElGamal 密码体制
答案：AD

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. 底层采用 SM4 算法的 EMAC，输出标签的比特长度支持（　）。
A.32
B.64
C.128
D.256
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. 为保证安全性，在设计分组密码时应该考虑（　）等问题。
A.在设计分组密码时，加密/解密变换必须足够复杂
B.加密时间要足够长
C.密钥空间足够大
D.解密时间要足够长
答案：AC

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. 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

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. 为保障分组密码工作模式的使用安全性，通常采用的措施有（　　）。
A.控制明文长度上限
B.经常更新加密密钥
C.多次加密同一明文
D.规范使用 Nonce、IV 等参数
答案：ABD

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. 评估 SM4 算法的安全性，必须考虑下述对分组密码算法常用的分析方法（　）。
A.差分分析
B.线性分析
C.不可能差分分析
D.积分分析
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. 混淆和扩散是密码设计的一般原则，所以在很多密码设计中，都采用了代换和置换等变化来达到混淆和扩散的效果。下列哪些密码体制中，采用了置换的处理思想？（　）
A.RSA
B.CAESAR 密码
C.AES
D.DES
答案：CD

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. 在对称分组密码 AES 中，共进行 10 轮迭代变换，第 10 轮进行了处理变换有（ ）。
A.字节代换
B.行移位
C.列混合
D.轮密钥加
答案：ABD

76. 盲签名与普通签名相比，其显著特点为（ ）。
A.签名者使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. 以下操作方式，可能出现安全问题的是（ ）。
A.使用 ECB 对于 RGB 图片进行加密
B.使用固定 IV 的 CBC 模式进行性别的加密
C.明文传递 CTR 模式的计数器值
D.未采用可靠方式传递根 CA 的自签名证书
答案：ABD

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. 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

90. 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

91. 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

92. 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

93. 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

94. 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

95. 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

96. 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

97. 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

98. 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

99. 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

100. 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

101. 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

102. 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

103. 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

104. 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

105. 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

106. 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

107. 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

108. 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

109. 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

110. 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

111. 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

112. 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

113. 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

114. 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 SM3withSM2Encryption 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

115. 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

116. 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

117. 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

118. 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

119. 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

120. 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

121. 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

122. 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

123. 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

124. 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

125. 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

126. 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

127. 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

128. 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

129. 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

130. 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

三、判断题 80
1.5G 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

2.AES 算法是一种分组密码算法，其分组长度固定为 128 比特。
答案：对

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.凯撒密码是一种典型的单表代换密码。
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.分组密码的 CTR 模式在解密时需要使用分组密码的解密算法。
答案：错

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.在分组密码的 ECB 模式下，相同的明文分组会被加密成相同的密文分组。
答案：对

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.RSA 算法的安全性基于椭圆曲线离散对数问题。
答案：错

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.数字签名可以实现对消息来源的认证，但不能提供消息的机密性保护。
答案：对

15.数字证书中的私钥可以公开，因为公钥是保密的。
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.SHA-256 算法的输出长度为 256 比特。
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.哈希函数可以用于加密消息，因为它是可逆的。
答案：错

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.SM4 算法是我国自主设计的分组密码算法，其分组长度为 128 比特，密钥长度为 128 比特。
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.SM2 数字签名算法生成的签名长度与 SM3 哈希值长度相同。
答案：错

27.量子计算对 RSA 和 ECC 公钥密码构成威胁，但对对称密码和哈希函数影响较小（通常需要增大密钥长度）。
答案：对

28.SHA-512 处理消息时，每个分组有 80 轮运算。
答案：对

29.在 Diffie-Hellman 密钥交换协议中，通信双方需要共享一个预先分配的秘密密钥。
答案：错

30.SM2 签名速率一般小于验签速率。
答案：错

31.格密码是一类被认为可以抵抗量子计算攻击的公钥密码候选算法。
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.消息认证码可以保证消息的机密性，因为只有持有密钥的人才能生成和验证。
答案：错

35.SM2 加密算法可以用来保护消息机密性。
答案：对

36.在公钥基础设施 PKI 中，数字证书用于将用户的身份与其公钥绑定。
答案：对

37.在 RSA 中，选择两个大素数 p 和 q，计算 n=pq，公钥(n,e)可以公开，私钥(n,d)中的 d 必须与 e 相等。
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.CCM 认证加密模式结合了 CTR 模式的机密性和 CBC-MAC 的完整性保护。
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.对密码系统进行暴力破解的难度只取决于密钥长度，与算法无关。
答案：错

43.密钥派生函数可以从一个主密钥和安全参数派生出多个子密钥。
答案：对

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.古典密码中的仿射密码是置换密码的一种。
答案：错

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.在 RSA 密码算法中，加密指数 e 和私钥指数 d 必须都小于模数 n 的欧拉函数 φ(n)。
答案：对

49.在分组密码的 CFB 模式下，解密过程与加密过程使用相同的分组密码操作，但需要反序使用密钥。
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.AES 算法的分组长度固定为 128 比特，密钥长度可以是 128、192 或 256 比特。
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.数字信封技术使用发送者的私钥加密对称密钥，使用接收者的公钥加密消息。
答案：错

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.对消息进行数字签名时，通常先对消息的哈希值进行签名，以提高效率。
答案：对

57.所有哈希函数都具有抗原像攻击、抗第二原像攻击和抗碰撞攻击的安全性。

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.CBC 模式在加密时需要初始化向量 IV，且 IV 必须随机且不可预测。
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.在公钥密码中，加密和解密使用相同的密钥，因此称为对称密码。
答案：错

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.序列密码的加密速度通常快于分组密码，适合数据流加密。
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.伪随机数发生器不需要种子即可生成随机数序列。
答案：错

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.密码学中的“混淆”和“扩散”概念由 Shannon 提出，用于衡量密码算法的安全性。

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

75.一次一密体制可以实现完全保密，因此可以同时保证消息的完整性和不可否认性。
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

四、填空题 30
1.基域选择 Fp-256 时，SM2 算法的数字签名的私钥长度为_____。
答案：256

2.某政务系统使用国密对称算法对敏感文件进行加密，该算法的分组长度为 128 位，密钥长度可为 128/192/256 位，且采用非平衡 Feistel 结构。该算法的标准名称是____。
答案：SM4

3.在金融 IC 卡应用中，使用基于椭圆曲线双线性对的标识密码算法实现无需证书的身份认证，该算法是____。
答案：SM9

4.MD5 算法输出 128 位哈希值，但已被证明存在碰撞攻击，不适用于数字签名

场景。我国 SM3 算法输出____位哈希值，安全性更高。
答案：256

5.SM4 国密分组密码算法的明文分组长度为 _____ 比特。
答案：128

6.SM3 算法的初始化向量 IV 为 7380166f 4914b2b9 172442d7 da8a0600 a96f30bc 163138aa e38dee4d b0fb0e4e，共____个 32 位字。
答案：8

7.有一张长长的数字“藏宝图”（消息），长度为 1000 字节。你需要用 SM3 算法计算它的“指纹”（杂凑值）。SM3 处理消息时，会把它切成若干个 512 位（64 字节）的块，那么可以切 16 块。

8.SM4 算法的加密迭代轮数为 _____ 轮。
答案：32

9.你需要用 SM4 算法加密一条信息，想象加密过程就像通过一个有 32 扇门的迷宫，每过一扇门，信息就会被转换一次，而且每扇门都需要一把不同的钥匙（轮密钥），那么加密一个消息，需要穿过这个迷宫的____扇门。
答案：32

10.当 AES 的明文分组和密钥长度均为 128 比特时，加密迭代轮数为 _____ 轮。
答案：10

11.SM2 是一种基于椭圆曲线密码的公钥加密算法，如果明文长度是 128 比特，那么经过 SM2 加密后的密文长度是_____比特。
答案：896

12.凯撒密码是一种经典的替换密码，通过将字母表中的每个字母移动固定的偏移量来进行加密。若给定偏移量为 3，明文字母'A'的密文字母是____。
答案：D

13.SM3 密码杂凑算法是中国国家密码管理局发布的一种密码杂凑算法，其压缩函数一共有_____种不同的布尔函数。
答案：2

14.3DES 算法的加密迭代轮数为 _____ 轮（16 轮×3）。
答案：48

15.DES 是一种广泛使用的对称密钥加密算法，其加密过程基于 Feistel 网络结构，共经过_____次迭代运算的处理。
答案：16

16.RSA 算法中，已被认为不安全、逐步淘汰的密钥长度为 _____ 比特。
答案：1024

17.维吉尼亚加密是一种经典的多表替代密码，由布莱斯·德·维吉尼亚在 16 世纪提出。它通过密钥对明文进行加密，增强了单表替代密码的安全性。给定明文 HELLO 和密钥 KEY，则加密后的密文是_____。
答案：RIJVS

18.你要和盟友交换 SM2 公钥。你告诉他，你发送的未压缩公钥字符串会以一个特殊的十六进制前缀“ _____”开头，这样他就能识别出来。
答案：04

19.SHA-256 算法输出的哈希值通常表示为 _____ 个十六进制字符。
答案：64

20.在 Diffie-Hellman 密钥交换协议中，双方使用公共参数：素数模数 p=23 和原根 g=5。Alice 选择私有密钥 a=6，Bob 选择私有密钥 b=15。根据协议，Alice 需要计算她的公钥 A 并发送给 Bob，那么 Alice 的公钥 A=____。
答案：8

21.对于 Hill 密码，给定密钥矩阵 K=$\begin{pmatrix} 11 & 8 \\ 3 & 7 \end{pmatrix}$ 和密文 DHFL（字母映射：A=0, B=1, ..., Z=25），则明文为_____。
答案：RQZC

22.在 SM2 公钥加密算法中，密文由 C1、C2 和 C3 三部分组成。如果 SM2 的密文长度是 2048 比特，那么相应明文长度是_____比特。
答案：1280

23.你有一条很短的消息，只有 1 字节（比如一个字母“A”）。为了用 SM3 计算它的杂凑值，必须进行填充，使其总长度是 512 位的倍数。那么对这 1 字节的消息进行 SM3 填充后，整个消息（原始消息+填充数据）的总长度是____比特。
答案：512

24.在(k,n)-秘密分割门限方案中，至少需要 _____ 个参与者才能重构被分割的秘密。
答案：k

25.在 RSA 密钥生成过程中，两个质数 p 和 q 被选中，已知它们的和 p+q=24 且积 p×q=143。那么，用于计算私钥的欧拉函数 ϕ（n）的值为____。
答案：120

26.假如你截获了一份文件，需要验证其真伪。你使用 SM3 算法为其生成一个唯一的“数字指纹”（杂凑值）。这个指纹的长度是____比特。
答案：256

27.SM4 分组密码算法采用 32 轮非线性迭代结构（Feistel 网络），每轮使用一个

轮密钥和一个固定的非线性变换。其加密过程共需要进行___轮非线性迭代运算。
答案：32

28.使用 SM2 算法加密一条长度为 16 字节的明文消息，若采用未压缩点形式表示公钥点，则最终生成的密文长度为____字节。
答案：113

29.假如你正在处理 SM4 加密的数据，知道 SM4 每次加密的数据块大小是固定的，就像保险箱的储物格一样大，每个格子可以存放___比特的数据。
答案：128

30.一段密文由栅栏密码加密所得，其解密过程如下：首先计算出栏数（密钥）为 4，然后将密文依次按列填入一个 4 列的栅栏中，最后按行读取得到明文。若密文长度为 19 个字符，则用于填充密文的栅栏矩阵，其最后一行的列数应为____。
答案：3

二、密码前沿技术 195

一、单选题 115
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.量子技术是基于量子力学基本原理发展而来的新一代颠覆性技术。以下关于量子技术三大核心概念的表述中，正确的是（　）
A. 量子技术的三大核心概念是叠加、纠缠和退相干
B. 量子技术的三大核心概念是叠加、纠缠和测量
C. 量子技术的三大核心概念是测量、退相干和干涉
D. 量子技术的三大核心概念是纠缠、干涉和不可克隆
答案：B

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.量子计算之所以具备显著超越经典计算的算力优势，其核心原因在于（　）
A. 量子计算机的时钟频率远高于经典计算机
B. 量子比特的叠加态特性使量子系统能够同时表征 2 的 N 次方个基态的组合状态
C. 量子计算机使用了更先进的半导体制造工艺
D. 量子计算机的存储容量是经典计算机的指数倍
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

7.一个量子比特（qubit）与一个经典比特（bit）的根本区别在于（　）
A. 量子比特只能处于 0 状态
B. 量子比特只能处于 1 状态
C. 量子比特可以同时处于 0 和 1 的叠加状态
D. 量子比特的物理尺寸比经典比特更小
答案：C

8.在量子力学中，两个纠缠的量子比特之间存在的关联特性，被称为（　）
A. 量子隧穿效应
B. 波粒二象性
C. “鬼魅般的超距作用”
D. 海森堡不确定性原理
答案：C

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.量子密钥分发（QKD）在数据安全保护中的独特优势在于（ ）
A. 其密钥生成速度比传统方法快得多
B. 其安全性建立在物理定律之上而非数学难题的复杂性之上
C. 其密钥长度是无限长的
D. 其不需要任何密钥管理
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 N 个量子比特的信息承载能力，以下说法正确的是（ ）
A. N 个量子比特可以同时表征 N 种状态
B. N 个量子比特可以同时表征 2N 种状态
C. N 个量子比特可以同时表征 2 的 N 次方种基态组合状态
D. N 个量子比特可以同时表征 N 的 2 次方种状态
答案：C

14.量子密钥分发（QKD）在实际部署中通常采用的方式是（ ）
A. 完全替代所有现有通信网络
B. 以“外挂”的方式叠加在现有通信网络上：先用量子信道生成密钥，再用密钥对信息加密传输
C. 仅在实验室环境中使用
D. 只用于无线通信
答案：B

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.量子世界中存在一条“铁律”：未知的量子态无法被精准复制。这一特性被称为（　）
A. 量子叠加原理
B. 量子不可克隆定理
C. 量子纠缠定理
D. 量子测不准原理
答案：B

17.量子密钥分发（QKD）之所以能够实现安全通信，其核心物理基础在于（　）
A. 量子比特的计算速度极快
B. 任何窃听或探测行为都会扰动量子态，使通信双方立刻察觉
C. 量子密钥的长度远超传统密钥
D. 量子通信不需要任何物理传输介质
答案：B

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.NIST 发布的抗量子密码标准 FIPS 203（ML-KEM）和 FIPS 204（ML-DSA）分别用于（　）
A. 两者都是数字签名标准
B. 两者都是密钥封装标准
C. ML-KEM 用于密钥封装，ML-DSA 用于数字签名
D. ML-KEM 用于数字签名，ML-DSA 用于密钥封装
答案：C

20.我国在抗量子密码领域的重要进展包括（　）
A. 已完成全部抗量子密码标准的制定并开始强制实施
B. 基于国产抗量子芯片完成了 AI 多智能体可信通信试验
C. 尚未开展抗量子密码相关研究工作
D. 只依赖国际标准，不进行自主研发
答案：B

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.当前量子科技的落地应用主要聚焦三大核心赛道，分别是（　）
A. 量子计算、量子通信与量子精密测量
B. 量子计算、量子存储与量子传感
C. 量子通信、量子雷达与量子成像
D. 量子精密测量、量子材料与量子生物
答案：A

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.以下哪项不属于五大抗量子密码技术路线？（　）
A. 基于格的密码
B. 基于编码的密码
C. 基于量子密钥分发的密码
D. 基于多变量的密码
答案：C

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.下列关于量子叠加态的表述，正确的是（　　）
A. 叠加态是指量子比特处于 0 和 1 之间的某个确定中间值
B. 叠加态是指量子比特在被观测前可以同时具有 0 和 1 的可能性
C. 叠加态只存在于理论推导中，尚未被实验证实
D. 叠加态一旦形成就无法改变
答案：B

27.我国自主研发的光量子计算原型机“九章四号”在执行高斯玻色取样任务时，生成一个样本仅需 25 微秒。该原型机可精准操纵的光子数量为（　）

A. 100 个
B. 1000 个
C. 10000 个
D. 100000 个
答案：C

28.量子计算在处理某些特定类型问题时展现出远超经典计算机的能力，但这种加速效应（　）
A. 对所有类型的问题都普遍适用
B. 只对特定类型的问题有效
C. 只对密码破解类问题有效
D. 只对人工智能训练有效
答案：B

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.后量子密码迁移被 Gartner 列为 2026 年六大网络安全趋势之一，其核心要求是（　）
A. 在量子计算机出现后再开始迁移
B. 加速识别、管理并替换传统加密体系，优先构建密码敏捷性
C. 只对金融行业进行密码迁移
D. 一次性完成所有系统的密码替换
答案：B

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.关于“加密敏捷性”（Crypto Agility）的概念，以下理解正确的是（　）
A. 指加密算法的运行速度足够快
B. 指系统架构具备快速替换和切换加密算法的能力
C. 指加密密钥可以随时更换
D. 指加密算法可以自我进化
答案：B

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.对抗量子计算威胁，保障信息安全的当前主流可行技术路线是（　）
A. 只依赖量子密钥分发（QKD）
B. 只增加传统加密算法的密钥长度
C. 部署抗量子密码（PQC）
D. 放弃所有加密，改用物理隔离
答案：C

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.抗量子密码迁移的困难通常以 10 年以上为单位推进，主要原因是（　）
A. 量子计算机尚未问世，无需着急
B. 抗量子密码算法尚未标准化
C. 企业必须确认系统相依性、应用相容性、凭证链、设备支援度等方面的合规要求
D. 抗量子密码算法运行速度太慢
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.在量子通信中，量子密钥信息通常编码在何种物理载体上进行传输？（　　）
A. 无线电波
B. 光纤中的经典光信号
C. 单光子、弱相干光脉冲或纠缠光子等量子态
D. 电流脉冲信号
答案：C

49.在量子计算时代，一种令人不安的新型攻击策略是“先存储、后解密”。这种攻击方式指的是（　）
A. 攻击者先破解加密算法再窃取数据
B. 攻击者现在截获并存储加密数据，待量子计算技术成熟后再批量解密
C. 攻击者先解密旧数据再攻击新系统
D. 攻击者先破坏密钥管理系统再窃取数据
答案：B

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.抗量子密码（Post-Quantum Cryptography, PQC）诞生的根本原因是（　　）
A. 经典计算机的算力已经足够破解现有密码
B. 量子计算技术的快速发展对基于大整数分解和离散对数难题的经典密码体系构成了颠覆性安全威胁
C. 现有密码算法的密钥长度不够长
D. 传统密码算法在经典计算机上的运行速度太慢
答案：B

52.目前全球已形成五大主流抗量子密码技术路线，其中综合表现最优、成为国际标准优先选用技术路线的是（　　）
A. 基于编码的密码
B. 基于哈希函数的密码
C. 基于格的密码
D. 基于同源的密码
答案：C

53.美国国家标准与技术研究院（NIST）首批发布的抗量子密码标准中，用于密钥封装的算法是（　　）
A. ML-DSA
B. FN-DSA
C. ML-KEM
D. SHA-256
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.根据相关预测，能够破解 RSA 和椭圆曲线加密（ECC）的量子计算机可能在多长时间内出现？（　）
A. 已经出现
B. 五年内
C. 五十年后
D. 永远不会出现
答案：B

56.关于 NIST 抗量子密码标准化进程，以下说法正确的是（　）
A. NIST 已完成全部标准化工作，不再有新算法进入评审
B. 2026 年 5 月，NIST 从第二轮评审中选出了 9 个候选算法进入第三轮
C. NIST 只评审基于格的密码算法
D. NIST 的抗量子密码标准化工作与量子计算机无关
答案：B

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.当前，后量子密码迁移普遍被业界建议视为（　　）
A. 一次性的“大切换”，应在短期内完成
B. 持续数年甚至十年的渐进工程
C. 仅在金融行业实施的专项工程
D. 可以无限期推迟的非紧急事项
答案：B

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.量子计算机对传统公钥密码体系的威胁主要来自（　）
A. Grover 算法
B. Shor 算法
C. Deutsch-Jozsa 算法
D. Simon 算法
答案：B

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.Shor 算法在理论上能够高效破解的传统密码算法类型是（　）
A. 仅对称加密算法如 AES
B. 仅哈希算法如 SHA-256

C. 基于大整数分解和离散对数难题的公钥密码算法如 RSA 和 ECC
D. 所有类型的密码算法
答案：C

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.量子计算机成熟后，以下哪些领域的数据安全将首当其冲面临威胁？（　）
A. 仅个人社交媒体数据
B. 金融交易、政府通讯、云端资料及关键基础设施
C. 仅公开的学术研究数据
D. 仅娱乐媒体内容
答案：B

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.Grover 算法对对称密码安全强度的影响是（　）

A. 使对称密码完全失效
B. 使对称密码的有效密钥长度减半
C. 对对称密码没有任何影响
D. 使对称密码的有效密钥长度加倍
答案：B

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

71.2026 年 3 月，谷歌发布的白皮书指出，破解 256 位椭圆曲线离散对数问题所需的物理量子比特数量约为（　　）
A. 53 个
B. 50 万个
C. 100 万个
D. 1000 个
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.关于量子计算对数据安全的影响，以下说法错误的是（　）
A. 量子计算机可能使 RSA 等传统公钥加密算法失效
B. “先存储、后解密”策略使长期敏感数据面临现实安全风险
C. 对称加密算法（如 AES）完全不受量子计算影响
D. 部署抗量子密码是守护数字安全的必然选择
答案：C

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.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

79.量子计算机成熟后，以下哪类加密算法被认为最可能首先失去防护能力？（　）
A. AES 对称加密算法
B. RSA 和 ECC 等传统公钥加密算法
C. 哈希算法
D. 流密码算法
答案：B

80.关于区块链的“51%攻击”，以下哪项描述是正确的？　（　）
A.攻击者需要控制全网超过 51%的算力，才能双花攻击或阻止交易确认
B.攻击者需要控制全网超过 51%的节点数量，才能篡改已确认的历史区块

C.51%攻击成功后，攻击者可以随意修改其他用户的私钥和资产余额
D.51%攻击在 PoS（权益证明）机制中完全不存在，因为 PoS 不依赖算力
答案：A

81.某大型金融机构的首席信息安全官正在评估量子计算对现有密码体系的威胁。他在内部报告中指出："量子计算对非对称密码和对称密码的威胁机制完全不同。"以下关于量子计算对不同类型密码算法威胁的描述中，正确的是（　　）
A. Shor 算法可破解 RSA 和 ECC，但对 AES 等对称密码无任何影响
B. Grover 算法可将对称密码的密钥搜索复杂度从 $O(2^n)$降为 $O(2^{n/2})$，使有效密钥长度减半
C. Shor 算法和 Grover 算法均可破解非对称密码，但对对称密码均无效
D. Grover 算法可破解 RSA 和 ECC，Shor 算法可削弱 AES 的安全性
答案：B

82.区块链网络中，以下哪种攻击利用的是"交易延展性"漏洞？（　）
A.Sybil 攻击
B.粉尘攻击
C.交易 ID 篡改攻击（如早期比特币中的交易延展性攻击）
D. 重放攻击
答案：C

83.某政务云平台计划将核心业务系统从 RSA-2048 证书迁移至抗量子密码算法。安全团队在技术选型会议上讨论："Shor 算法对经典公钥密码构成了根本性威胁，其核心能力在于高效求解哪类数学问题？"以下选项正确的是（　　）
A. 大整数分解和离散对数问题
B. 格上的最短向量问题
C. 随机线性码的译码问题
D. 多变量二次方程求解问题
答案：A

84.智能合约安全中，"重入攻击"（Reentrancy）的典型防御措施是？（　　）
A.使用 require 检查调用者余额
B.先更新合约内部状态，再调用外部合约
C.使用 assert 确保交易 Gas 充足
D. 限制合约调用的次数上限
答案：B

85.关于区块链节点之间的 P2P 网络，以下哪种安全威胁最为直接相关？（　　）
A.SQL 注入
B.Eclipse 攻击（日蚀攻击）
C.XSS 跨站脚本攻击
D. 缓冲区溢出
答案：B

86.某密码学会议上，一位专家在报告中指出："量子保密通信的安全性保障机制

与经典密码完全不同。”以下关于量子保密通信（量子密钥分发，QKD）安全性来源的描述中，正确的是（　　）
A. 其安全性基于大整数分解的计算复杂性
B. 其安全性基于离散对数的计算困难性
C. 其安全性基于量子力学基本原理，如未知量子态不可克隆定理和海森堡不确定性原理
D. 其安全性基于格上最短向量问题的求解困难性
答案：C

87.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

88.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

89.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

90.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

91.区块链中的零知识证明（ZeroKnowledge 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

92.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

93.BB84 协议是最早的量子密钥分发协议之一，由 Bennett 和 Brassard 于哪一年提出，其信息编码载体是什么？（　　）
A. 1994 年，利用光子的相位编码信息
B. 1984 年，利用光子的偏振状态编码信息
C. 1996 年，利用量子纠缠编码信息
D. 2016 年，利用量子比特的叠加态编码信息
答案：B

94.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

95.依据《网络安全标准实践指南——OpenClaw 类智能体部署使用安全指引》，个人使用者在部署 OpenClaw 类智能体时，建议优先选择哪种部署环境？（　　）
A.日常使用的终端环境
B.云环境
C.移动设备环境
D.离线环境
答案：B

96.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

97.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

98.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

99.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

100.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

101.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

102.依据《网络安全标准实践指南——OpenClaw 类智能体部署使用安全指引》，未经组织审批、部署、监控与管理，由员工个人在组织终端、服务器或办公环境中自行安装、运行的智能体实例被称为？（　　）
A.独立智能体
B.影子智能体
C.私有智能体
D.临时智能体
答案：B

103.根据《智能体规范应用与创新发展实施意见》，智能体被定义为具备自主感知、记忆、决策、交互与执行能力的智能系统。以下哪项不属于《实施意见》明确的智能体发展基本原则（　　）
A. 安全可控
B. 规范有序
C. 效率优先
D. 应用牵引
答案：C

104.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

105.《智能体规范应用与创新发展实施意见》提出要构建分类分级治理框架。对于敏感领域及重点行业，由网信部门联合行业主管部门实行备案、检测、问题产品召回等管理措施；对于部分生活娱乐、日常办公等低风险领域，则主要通过以下哪种方式实现高效治理（　　）
A. 事前行政审批
B. 全面禁止，待技术成熟后再开放
C. 合规自测、信息报告、分发平台管理、行业自律
D. 全部交由市场自主调节，无需任何监管
答案：C

106. 为防范智能体安全风险，《智能体规范应用与创新发展实施意见》强调要提升内生安全能力、加强供应链安全并化解应用衍生风险。以下哪项属于《实施意见》中提到的防范应用衍生风险的具体措施（ ）
A. 强制所有智能体必须接入国家统一身份认证平台
B. 完善常态化风险识别、预警及干预机制，强化人机协同审核与拦截阻断
C. 禁止智能体在公共场所使用，以杜绝潜在风险
D. 要求所有智能体开发者将源代码交由监管部门托管
答案：B

107.某密码学课程讨论量子计算对经典密码体系的威胁程度。以下关于量子计算威胁的表述中，最准确的是（　　）
A. 量子计算机将破解所有现有密码，整个互联网安全体系将彻底崩塌
B. 量子计算主要威胁 RSA.ECC 等非对称密码，对对称密码的威胁相对有限且可通过增大密钥长度应对
C. 量子计算只威胁对称密码，不威胁非对称密码
D. 量子计算对密码体系没有任何实质性威胁，只是理论上的担忧
答案：B

108.某安全公司正在开发抗量子密码产品，需要为不同安全级别的应用场景选择合适的算法参数。NIST 标准化的抗量子密码算法都提供了多组不同的参数选项。以下关于这一设计的理解中，正确的是（　　）
A. 不同参数可达到不同的安全级别，使用者可根据应用需求选择
B. 不同参数仅影响算法运行速度，不影响安全性
C. 所有参数的安全性完全相同，只是密钥格式不同
D. 参数选择由 NIST 强制指定，使用者无权选择
答案：A

109.某大型企业的安全团队正在评估“迁移到抗量子密码的时间窗口”。团队需要向管理层解释：为什么不能等到量子计算机真正具备破解能力再开始迁移。以下关于迁移紧迫性的解释中，正确的是（　　）
A. 因为量子计算机将在明年就具备破解能力
B. 因为向后量子密码学过渡需要数年时间，且“先存储、后解密”已构成现实风险
C. 因为经典密码算法将在明年全部失效
D. 因为抗量子密码算法的部署只需要一天时间
答案：B

110.某跨国企业的安全架构师正在制定从经典密码向抗量子密码迁移的路线图。该企业拥有庞大的 PKI 基础设施，无法在短期内完成全面替换。以下关于抗量子密码迁移策略的描述中，正确的是（　　）
A. 应等到量子计算机真正具备破解能力后再开始迁移
B. 抗量子密码的部署只需要升级软件，不需要更换硬件
C. 迁移只需替换非对称密码算法，对称密码无需任何调整
D. 可采用“传统密码+抗量子密码”混合模式，实现平滑过渡
答案：D

111.某安全研究员在分析量子计算对密码体系的威胁时，需要区分不同量子算法的攻击目标。以下关于 Shor 算法与 Grover 算法攻击目标的配对中，正确的是（　　）
A. Shor 算法→对称密码，Grover 算法→非对称密码
B. Shor 算法→非对称密码，Grover 算法→对称密码
C. Shor 算法→哈希函数，Grover 算法→数字签名
D. Shor 算法→密钥分发，Grover 算法→公钥加密
答案：B

112.某公司的密码学团队在研究格密码的原理。他们需要理解格密码的核心数学困难问题。以下关于格密码所依赖的困难问题的描述中，正确的是（　　）
A. 格密码的主要数学基础是格的最短向量问题（SVP）和最近向量问题（CVP）
B. 格密码仅依赖于大整数分解问题
C. 格密码依赖于椭圆曲线上的离散对数问题
D. 格密码依赖于随机线性码的译码问题
答案：A

113.某密码学教材中写道："格密码是抗量子密码中最有前景的技术路线之一。"以下关于格密码优势的描述中，不正确的是（　）
A. 格密码可以实现加密、数字签名、密钥交换等多种密码功能
B. 格密码的安全性依赖于求解格中问题的困难性
C. 格密码的密钥尺寸在所有抗量子密码路线中都是最小的
D. 格密码在安全性、公私钥大小和计算速度上可达到较好的平衡
答案：C

114.某密码学研究人员在论文中写道："基于哈希的签名方案是抗量子密码中理论安全性最强的一类。"以下关于基于哈希的签名方案特点的描述中，正确的是（　）
A. 基于哈希的签名方案可以实现公钥加密和密钥封装功能
B. 基于哈希的签名方案的安全性依赖于哈希函数的单向性等性质，如果哈希函数被攻破可以替换
C. 基于哈希的签名方案签名体积小，适合资源受限设备
D. 基于哈希的签名方案均为无状态方案，易于部署
答案：B

115.某政府部门需要存储一批保密期限为 30 年的核心涉密数据。安全专家建议："考虑到量子计算的远期威胁，即使现在使用 RSA-2048 加密存储也不足够安全。"以下关于这一建议理由的解释中，正确的是（　）
A. RSA-2048 现在已经被经典计算机破解
B. "先存储、后解密"攻击方式下，攻击者可先存储加密数据，待量子计算机成熟后再解密
C. RSA-2048 的密钥太短，经典计算机可在几年内暴力破解
D. 量子计算机现在已经能够破解 RSA-2048
答案：B

二、多选题 60
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. 量子技术的三大核心概念包括（　　）
A. 叠加
B. 纠缠
C. 测量
D. 退相干
答案：ABC

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. 以下关于量子比特特性的描述中，正确的有（ ）
A. 一个量子比特可以同时处于 0 和 1 的叠加状态
B. N 个量子比特可以同时表征 2 的 N 次方个基态的组合状态
C. 量子比特在被测量时会“坍缩”到某一个确定的结果
D. 量子比特的物理状态与经典比特完全相同
答案：ABC

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. 以下关于量子纠缠的描述中，正确的有（　　）
A. 两个纠缠的量子比特无论相隔多远，对其中一个的测量会瞬间影响另一个的状态
B. 量子纠缠是量子通信实现超远距离传输的核心基础
C. 量子纠缠效应受光速限制
D. 量子纠缠已被实验证实
答案：ABD

14. 面对量子计算对数据安全的威胁，企业和组织应采取的措施包括（　　）
A. 建立完整的加密资产盘点机制
B. 导入具备加密敏捷性的架构
C. 优先针对高敏感数据进行 PQC 防护验证
D. 等待量子计算机真正出现后再采取行动
答案：ABC

15. 量子计算对数据安全构成的威胁主要体现在（　　）
A. Shor 算法可高效破解 RSA 和 ECC 等公钥密码
B. Grover 算法可使对称密码的有效密钥长度减半
C. “先存储、后解密”策略使长期敏感数据面临泄密风险
D. 量子计算机可以破解所有类型的加密算法
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. 以下属于 NIST 已发布或正在推进的抗量子密码标准/候选算法的有（　　）
A. ML-KEM
B. ML-DSA
C. FN-DSA
D. FAEST、HAWK、MAYO 等
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. 以下属于五大抗量子密码技术路线的有（　）
A. 基于格的密码
B. 基于编码的密码
C. 基于哈希函数的密码
D. 基于量子密钥分发的密码
答案：ABC

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. 后量子密码迁移过程中，企业面临的主要挑战包括（　　）
A. 系统相依性的确认
B. 应用相容性的验证
C. 凭证链和设备支援度的评估
D. 运维流程与合规要求的适配
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. 关于量子密钥分发（QKD）的特性，以下说法正确的有（　　）
A. 基于量子不可克隆定理，光子无法被完整复制
B. 窃听行为会引入可观测的误码率，可被通信双方察觉
C. QKD 的安全性建立在物理定律之上
D. QKD 可以完全替代所有传统加密方法
答案：ABC

28. 我国在抗量子密码与数据安全领域取得的重要进展包括（　　）
A. 基于国产抗量子芯片完成了 AI 多智能体可信通信试验
B. 发布了国密+抗量子密码“双保险”混合架构的平滑迁移方案
C. 在“本源悟空”量子计算机上搭载了抗量子攻击密码防护体系
D. 已完成全球所有抗量子密码标准的制定
答案：ABC

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

31. 以下哪些是区块链共识机制中可能面临的安全风险或攻击？（　　）
A. Nothing-at-Stake（无利害关系）问题
B.长程攻击（Long-Range Attack）
C.短程重组攻击（Short-Range Reorg）
D.预映像攻击（Preimage Attack）
答案：ABC

32. 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

33. 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

34. 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

35. 针对区块链钱包的网络安全防护，以下哪些措施是有效的？（　）
A.使用硬件钱包（冷钱包）存储大额私钥
B.定期备份助记词，并存储在云端加密保险箱
C.在交易签名前，对交易内容进行二次确认（如显示完整接收地址）

D.避免使用同一地址多次接收转账，以增强隐私保护
答案：ACD

36. 某大型金融机构计划在 2030 年前将其公钥基础设施（PKI）迁移至抗量子密码体系。安全总监查阅了 Shor 算法的最新工程实现文献。关于 Shor 算法对现行密码体制的实际威胁，以下描述正确的有（　　）。
A. 破解 2048 位 RSA 密钥，在理想逻辑量子比特下约需数千万次量子门操作，且所需逻辑量子比特数约为密钥长度的两倍（约 4096 个）。
B. Shor 算法在量子计算模型下解决整数分解问题的时间复杂度相对于密钥长度是亚指数级的，因此其威胁远大于经典计算下的指数级攻击。
C. 攻击同等安全强度（128 bit 安全）的椭圆曲线密码（ECC-256）时，Shor 算法所需的逻辑量子比特数通常少于攻击 RSA-2048 所需的数目。
D. Shor 算法的核心数学变换依赖于量子傅里叶变换（QFT）来寻找周期，该周期寻找能力对离散对数问题同样有效，因此对 DSA 和 ECDSA 签名体制构成同等威胁。
答案：ACD

37. 某科研机构正在评估容错量子计算机（FTQC）的工程可行性。工程师指出，现有的超导量子比特退相干时间极短。关于量子纠错码（QECC）与表面码（Surface Code）的特性，下列说法正确的有（　　）。
A. 表面码的容错阈值约为 1%，这意味着物理量子比特的错误率必须低于该阈值，增加码距（Distance）可同时提升纠错能力和降低逻辑错误率。
B. 在表面码中，逻辑量子比特的数量远远大于物理量子比特的数量（即 Overhead < 1），因此工程上容易实现大规模量子计算。
C. 量子纠错面临“错误简并”问题（不同的 Pauli 错误导致相同的测量症状），这是经典纠错中不存在的独特挑战。
D. 为运行 Shor 算法分解 2048 位 RSA，若物理量子比特门保真度为 99.9%，通常估计需要数百万物理量子比特，主要原因就是纠错开销（Overhead）。
答案：ACD

38. 某政务系统需采用抗量子数字签名算法，评估了 ML-DSA（原 Dilithium）。密码分析师指出，Dilithium 使用了“拒绝采样”（Rejection Sampling）技术。关于 ML-DSA 的设计原理，正确的是（　　）。
A. ML-DSA 的安全性基于 M-SIS（Module Short Integer Solution）和 MLWE 问题的困难性，属于格基数字签名算法。
B. 拒绝采样技术的主要作用是消除私钥和随机盲化因子在签名输出中留下的正态分布尾部信息，防止通过大量签名样本反推出私钥（侧信道/统计攻击）。
C. Dilithium 采用了“Flat-Shamir with Aborts”范式，即先构造非交互式零知识证明（NIZK），若生成的签名多项式系数过大则丢弃重试，以保证输出服从均匀分布。
D. ML-DSA 的签名长度和公钥尺寸均明显小于基于哈希的 SPHINCS+，但其安全性依赖于量子计算机无法解决的格归约问题，属于有状态签名算法。
答案：ABC

39. 某物联网公司无法在设备上保存每次签名的状态计数器，因此排除了基于哈希的有状态签名，转而关注 SLH-DSA（原 SPHINCS+）。关于 SLH-DSA 的设

计特点，正确的有（　）。
A. SLH-DSA 是一种无状态（Stateless） 的基于哈希函数的数字签名方案，其安全性仅依赖于哈希函数的抗碰撞（Collision Resistance）性和抗原像性，与数论难题无关。
B. SLH-DSA 使用 Merkle 树来聚合大量一次性签名（OTS）公钥，并利用 WOTS+（Winternitz OTS+） 来缩短签名长度，但在每次签名时仍需生成新的 OTS 密钥对。
C. 由于 SLH-DSA 不涉及大整数运算和格点运算，其签名和验签速度极快，且公钥和私钥尺寸极小，适合资源受限的微控制器。
D. SLH-DSA 虽然提供了极高的量子安全性（保守），但其签名长度（通常几十 KB）远大于 ML-DSA 和 Falcon，这是其主要性能短板。
答案：ABD

40. 某备份系统拟采用基于编码的 McEliece 密码体制作为长期归档数据的加密方案，以应对远期量子威胁。关于 McEliece 体制（Classic McEliece）的特点，正确的有（ ）。
A. McEliece 的安全性建立在一般线性码的译码问题（Syndrome Decoding） 的 NP 困难性上，该问题在量子计算下缺乏有效的多项式时间解法。
B. Classic McEliece 使用不可约二元 Goppa 码作为陷门，通过随机置换生成码字，攻击者由于不知道置换和生成矩阵结构，无法有效译码。
C. McEliece 方案的公钥尺寸极大（通常数百 KB 至 1MB 以上），这是其未被广泛应用的主要原因之一，但其加密和解密速度极快，优于基于格的 KEM。
D. McEliece 方案存在极低的解密失败率（DFR，Decryption Failure Rate），在标准参数下 DFR 不为零，这在密钥封装中可能被利用进行适应性选择密文攻击（CCA）。
答案：ABC

41. 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

42. 依据《网络安全标准实践指南——OpenClaw 类智能体部署使用安全指引》，个人使用者在配置 OpenClaw 类智能体时，以下哪些安全措施是建议采取的？（　）
A.配置非公网暴露的端口，防止未授权调用
B.从官方仓库或可信来源获取 Skills
C.建立白名单机制，仅允许白名单中的 Skills、插件、MCP 等被调用
D.为高风险操作增加人工确认机制
答案：ABCD

43. 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

44. 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

45. 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

46. “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

47. 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

48. 《智能体规范应用与创新发展实施意见》围绕智能体创新发展部署了多项重点工作，以体系化推动智能体技术突破和生态建设。以下属于《实施意见》提出

的夯实发展基础具体举措的有（　　）。
A. 强化基础技术研发，加强智能体任务理解、任务规划、工具使用等技术攻关
B. 建立智能体标准体系，加快制定智能体与软件工具、应用服务等接口标准
C. 布局发展智能互联网，探索建立智能体注册平台，提供数字身份管理服务
D. 明确仅限用户本人决策、需授权决策和自主决策的合理边界，确保用户最终决策权
答案：ABC

49. 《智能体规范应用与创新发展实施意见》提出了“强化应用牵引”的举措，旨在通过典型场景应用牵引技术迭代。下列选项中，属于《实施意见》明确的智能体典型应用方向包括（　　）。
A. 智能制造：研发生产管理智能体，优化生产排程和资源分配
B. 医疗健康：探索药品管理、手术排程、病历管理等智能体，提升医疗服务效率
C. 金融服务：研发金融风控智能体，提升信贷审批、交易监控等环节风险识别能力
D. 教育教学：依托智能体开展个性化学习方案制定，完善智能导学与答疑辅导功能
答案：ABCD

50. 根据《人工智能应用伦理安全指引 1.0》，关于人工智能应用伦理安全原则，以下表述正确的有（ ）
A. 增进人类福祉原则要求人工智能应用应以促进社会公平正义和可持续发展为宗旨。
B. 确保可控可信原则要求确保人工智能的运行始终处于人类控制之下，防范其脱离人类监督。
C. 保护隐私安全原则仅要求在人工智能数据采集阶段做好隐私保护，不涉及数据使用和存储环节。
D. 坚持公平公正原则要求人工智能应用应避免对特定群体产生歧视性影响，保障机会均等。
答案：ABD

51. 某金融科技公司近期上线了客户信用评分系统，系统需实时调取央行征信、社保、电商消费等多源数据。数据安全官在制定数据分级策略时，应遵循哪些基本原则（　　）
A. 按数据破坏后的影响对象（个人、企业、公共利益）划分等级
B. 仅依据数据量大小确定安全级别，数据量越大级别越高
C. 结合数据生命周期各阶段（采集、存储、使用、销毁）动态调整级别
D. 分级结果应报监管部门审批后方可生效
答案：AC

52. 某跨国零售企业在中国境内运营，其数据中心位于新加坡，但涉及中国公民的会员消费记录、人脸支付特征。该企业数据保护官在判断法律适用时，哪些说法正确？
A. 因数据中心在境外，可不适用中国《中华人民共和国数据安全法》
B. 处理中国境内自然人个人信息，适用《中华人民共和国个人信息保护法》

C. 重要数据出境需通过国家网信部门组织的安全评估
D. 人脸特征属于敏感个人信息，出境需单独取得个人单独同意
答案：BCD

53. 某数据中台项目采用差分隐私技术对用户行为数据进行加噪发布，以支持宏观统计。关于差分隐私的应用，以下理解正确的是（　　）。
A. 加噪后数据无法反推个体，因此可任意公开无需脱敏
B. 差分隐私通过添加拉普拉斯或高斯噪声实现隐私保护
C. 隐私预算 ε 越小，保护强度越高但数据可用性越低
D. 差分隐私能完全抵御差分攻击，达到绝对安全
答案：BC

54. 某政府大数据平台遭受勒索软件攻击，攻击者加密了备份数据并索要赎金。事后复盘发现备份策略存在缺陷。关于数据备份与恢复的合规技术措施，正确的是（　　）。
A. 备份数据应与生产数据存储在同一阵列，以提高恢复速度
B. 应定期进行备份数据恢复演练，验证可用性
C. 采用“3-2-1”备份原则（3 份副本、2 种介质、1 份异地）
D. 备份数据可长期保留在同一物理位置，便于管理
答案：BC

55. 某云服务商向客户提供数据库加密功能，客户可选择应用层加密或透明数据加密（TDE）。关于两种方式的比较，正确的是（　　）
A. TDE 对应用透明，无需修改代码，适用于业务改造受限场景
B. 应用层加密可对字段级细粒度控制，但密钥管理复杂度高
C. TDE 加密后的备份文件和日志文件也自动被加密
D. 应用层加密无法防御具备数据库管理员权限的内部攻击
答案：ABC

56. 某企业实行数据安全岗位责任制，任命了数据安全负责人、数据保护官（DPO）及各部门数据安全专员。关于岗位职责划分，正确的是（　　）
A. DPO 应独立于业务部门，直接向最高管理层汇报
B. 数据安全负责人负责制定整体策略，DPO 负责监督合规
C. 数据安全专员由业务部门兼任，无需接受专业培训
D. 发生数据泄露时，DPO 需在法定时限内向监管机构报告
答案：ABD

57. 某 AI 训练平台使用 Web 爬虫抓取公开网页上的用户评论数据，用于情感分析模型。关于爬取公开数据的合规边界，以下说法正确的有（　　）
A. 公开数据可随意爬取，不受《中华人民共和国个人信息保护法》约束
B. 即使数据公开，若包含个人信息，仍需评估处理合法性基础
C. 应遵守网站的 robots.txt 协议，避免过度请求
D. 爬取的数据可用于任何商业目的，不受限制
答案：BC

58. 某公司采购了一套数据防泄漏（DLP）系统，部署在网络出口和终端。关于

DLP 系统有效配置的策略，正确的有（　　）。
A. 基于正则表达式匹配身份证、银行卡等模式，阻断外发
B. 对加密压缩包无法检测，因此不需要监控压缩文件
C. 应结合内容指纹和上下文（如文件密级）综合判断
D. 可对内部邮件、即时消息、云盘上传等通道进行监控
答案：ACD

59. 某金融机构计划将客户风险评级模型外包给第三方科技公司开发，模型需使用脱敏后的客户交易数据。关于第三方数据委托处理的安全要求，正确的是（　　）。
A. 双方应签订数据处理协议，明确处理目的、期限、方式
B. 委托方对受托方的数据处理活动负有监督责任
C. 受托方可直接将数据转委托给其子公司，无需告知委托方
D. 模型开发完成后，受托方应按照约定删除或返还所有数据
答案：ABD

60. 某电商平台发生内部员工越权导出大量用户订单信息，并售卖至黑市。事后审计发现权限管理存在漏洞。关于权限管理与访问控制，正确的有（　　）
A. 应采用最小权限原则，仅授予岗位必需的最小数据访问范围
B. 应定期复审员工权限，离职人员需及时回收
C. 高敏感数据操作应启用双人授权或二次审批流程
D. 所有员工默认拥有查看全部数据的权限，再根据违规行为单独回收
答案：ABC

三、判断题 20
1. 区块链的不可篡改性意味着一旦交易上链，就绝对不可能被撤销或修改。
答案：错

2. 在区块链网络中，使用 TLS/HTTPS 加密节点之间的通信可以完全防止中间人攻击和 Sybil 攻击。
答案：错

3. 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

4. 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

5. 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

6. 依据《网络安全标准实践指南——OpenClaw 类智能体部署使用安全指引》，卸载 OpenClaw 类智能体后，无需对残留数据、密钥、凭证等进行清理，因为卸载程序会自动完成所有清理工作。
答案：错

7. 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

8. 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

9. 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

10. 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

11. 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

12. 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

13. 依据《网络安全标准实践指南——OpenClaw 类智能体部署使用安全指引》，卸载 OpenClaw 类智能体后，无需对残留数据、密钥、凭证等进行清理，因为卸载程序会自动完成所有清理工作。
答案：错

14. 根据《人工智能应用伦理安全指引 1.0》，人工智能应用可能带来“人类主导权影响”，即人工智能行为超出人类所预设、理解和可控的范围，可能冲击人类在社会运行和治理过程中的主导地位。
答案：对

15. 根据《智能体规范应用与创新发展实施意见》，对于部分生活娱乐、日常办公等低风险领域的智能体应用，应采取与敏感领域和重点行业相同的管理措施，即实行备案、检测、问题产品召回等严格管理方式。
答案：错

16. 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

17. 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

18. 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

19. 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

20. 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

三、标准题 245

一、单选题 90
1. GM/T 0111-2021《区块链密码应用技术要求》的适用范围是以下哪一项 （ ）
A. 公有区块链的密码应用技术要求
B. 私有区块链的密码应用技术要求
C. 联盟区块链的密码应用技术要求
D. 所有类型区块链的密码应用技术要求
答案：C

2. GM/T 0129-2023《SSH 密码协议规范》规定的 SSH 密码协议由哪三个子协议构成？ （ ）
A. 传输层协议、鉴别协议、连接协议
B. 传输层协议、会话协议、管理协议
C. 密钥交换协议、加密协议、认证协议
D. 握手协议、记录协议、警报协议
答案：A

3. 根据 GM/T 0129-2023《SSH 密码协议规范》，以下关于该标准中密码算法要求，说法正确的是？ （ ）
A. 非对称密码算法必须采用 RSA 算法，SM2 为可选
B. SM4-CBC 模式是必选的对称加密模式，SM4-GCM 为可选
C. 完整性校验使用 SHA-256 算法，SM3 为可选
D. 所有密码算法均为可选，由用户自行决定
答案：B

4. GB/T 17964-2021《信息安全技术 分组密码算法的工作模式》描述的九种工作模式，其主要用途是 （ ）
A. 保护数据的完整性和机密性
B. 保护数据的机密性

C. 保护数据的完整性和可用性
D. 保护数据的不可否认性
答案：B

5. 以下哪种分组密码工作模式存在“相同明文分组加密后得到相同密文分组”的特性，因而不推荐单独使用 （ ）
A. CBC（密文分组链接模式）
B. ECB（电码本模式）
C. CTR（计数器模式）
D. CFB（密文反馈模式）
答案：B

6. 根据 GB/T 17964-2021《信息安全技术 分组密码算法的工作模式》，该标准正文中描述了九种分组密码工作模式。以下哪项是标准中不包含的工作模式（ ）
A. XTS（带密文挪用的 XEX 可调分组密码模式）
B. HCTR（带泛杂凑函数的计数器模式）
C. GCM（伽罗瓦计数器模式）
D. OFBNLF（带非线性函数的输出反馈模式）
答案：C

7. 根据 GM/T 0021—2023《动态口令密码应用技术规范》，关于种子密钥（Seed Key）的管理，以下哪项说法是正确的 （ ）
A. 种子密钥可由制造方生成，并直接安装在动态口令令牌中，密钥管理中心仅负责存储备份
B. 种子密钥的生命周期包含“产生、待激活、可用、过期、销毁”五个阶段，其有效期应不大于 15 年（180 个月）
C. 种子密钥的长度应不小于 128 比特，应使用符合要求的随机数发生器生成
D. 种子密钥管理系统可设置在制造方，以便于令牌生产时直接写入种子密钥
答案：C

8. 根据 GB/T 45654-2025《网络安全技术 生成式人工智能服务安全基本要求》，数据来源选择时，经评估数据内容中含违法不良信息情况超过多少比例的，不应对该数据来源进行采集？（ ）
A.3%
B.5%
C.10%
D.15%
答案：B

9. 根据 GB/T 45654-2025《网络安全技术 生成式人工智能服务安全基本要求》，生成内容安全性方面，应保证模型生成内容合格率不低于多少？（ ）
A.80%
B.85%
C.90%
D.95%

答案：C

10. 根据 GB/T 46800-2025《生成式人工智能技术应用社会影响评估指南》，社会影响评估框架不包括以下哪个方面？（ ）
A.对个体与群体的影响
B.对组织与行业的影响
C.对经济社会系统的影响
D.对技术性能的影响
答案：D

11. 根据 GB/T 17901.3-2021《信息技术 安全技术 密钥管理 第 3 部分：采用非对称技术的机制》，在公钥传递机制中，实体 A 的公钥传递方式应符合以下哪项描述？（ ）
A. 实体 A 的公钥必须加密后传给其它实体
B. 实体 A 的公钥经鉴别后传给其它实体，但不需保密
C. 实体 A 的公钥不经鉴别直接公开广播
D. 实体 A 的公钥通过对称加密方式传给实体 B
答案：B

12.根据 GB/T 17901.1-2020《信息技术 安全技术 密钥管理 第 1 部分：框架》，以下哪项内容不属于该标准所包含的范围？（ ）
A. 建立密钥管理机制的通用模型
B. 定义对 GB/T 17901 通用的密钥管理基本概念
C. 规定具体密码算法的实现细节
D. 规定对密钥在其生存周期内进行管理的通用原则
答案：C

13.根据 GM/T 0074—2019《网上银行密码应用技术要求》，该标准所规定的密码技术在网上银行业务中应用的相关要求，不包含以下哪一项？（ ）
A. 密码算法
B. 证书管理
C. 密钥管理
D. 密码模块物理防护等级
答案：D

14.根据 GM/T 0074—2019《网上银行密码应用技术要求》，在密码功能要求中，为保证客户与网银系统双方交易活动的抗抵赖性，应对活动信息进行以下哪项处理？（ ）
A. 加密传输
B. 数字签名
C. 杂凑运算
D. 消息鉴别码计算
答案：B

15.根据 GM/T 0074—2019《网上银行密码应用技术要求》，以下哪项业务类型中，对公客户和个人客户均不需要密码技术提供抗抵赖性保护？（ ）

A. 查询业务
B. 资金变动业务
C. 签约业务
D. 其他业务
答案：A

16.根据 GM/T 0025—2023《SSL VPN 网关产品规范》，关于设备自检要求，以下哪项属于必选项？
A. CPU、内存等物理部件检查
B. 硬件功能模块正确性检测
C. 算法正确性、密钥完整性、随机数可靠性检测
D. 网络接口功能检测
答案：C

17.根据 GM/T 0025—2023《SSL VPN 网关产品规范》，关于 SSL VPN 网关产品的可靠性要求，平均无故障工作时间应不低于多少小时？
A. 5000 小时
B. 8000 小时
C. 10000 小时
D. 15000 小时
答案：C

18.根据 GM/T 0108—2021《诱骗态 BB84 量子密钥分配产品技术规范》，该标准基于以下哪种协议对量子密钥分配产品的技术实现进行规范？
A. 基于纠缠态的 E91 协议
B. 基于连续变量的 CV-QKD 协议
C. 采用弱相干态光源的诱骗态 BB84 协议
D. 采用单光子源的 BB84 协议
答案：C

19.根据 GM/T 0032—2014《基于角色的授权管理与访问控制技术规范》，该标准中负责对访问请求做出判定功能的部件是？
A. 访问控制执行部件（AEF）
B. 访问控制决策部件（ADF）
C. 属性管理系统
D. 权限管理中心
答案：B

20.某应用系统开发商正在为客户开发一套基于角色的授权管理功能。客户的人力资源部门需要定义公司员工（主体）与各业务角色（如财务主管、人事专员等）之间的分配关系。开发人员需要明确这种分配关系的描述语言应由谁来负责实现根据 GM/T 0032—2014《基于角色的授权管理与访问控制技术规范》，授权策略描述语言（定义主体与角色间的分配关系）应由以下哪方实现？
A. 应用系统开发商
B. 访问控制产品开发商
C. 用户单位的权限主管部门（如人力资源部门）

D. 密码设备制造商
答案：C

21.某大型企业部署了基于角色的授权与访问控制系统，系统包含多种功能部件。其中，访问控制决策部件（ADF）收到一个来自某员工的访问请求后，结合该员工的授权信息和资源的访问控制策略进行评估，最终做出是否允许访问的判定。根据 GM/T 0032—2014《基于角色的授权管理与访问控制技术规范》，ADF 的判定结果包括以下哪两种？
A. 允许和待确认
B. 允许和拒绝
C. 通过和驳回
D. 授权和禁止
答案：B

22.某电子政务系统采用基于标识的密码技术（IBC）实现用户身份鉴别。系统在设计中需要明确标识（identity）的定义，以便统一用户身份数据的格式。根据 GM/T 0057—2018《基于 IBC 技术的身份鉴别规范》，以下关于“标识”的表述，正确的是哪一项？
A. 标识必须是用户的电子邮箱地址
B. 标识必须是用户的手机号码
C. 标识是能够确定一个对象身份的唯一信息，例如电子邮箱地址、手机号码、指纹数据等
D. 标识是指用户的姓名和身份证号码
答案：C

23.某应用系统正在开发身份鉴别功能。系统开发人员需要查阅 GM/T 0057 标准的相关技术要求。根据 GM/T 0057—2018《基于 IBC 技术的身份鉴别规范》，该标准依托于以下哪项算法？
A. SM2 椭圆曲线公钥密码算法
B. SM3 杂凑算法
C. SM4 分组密码算法
D. SM9 标识密码算法
答案：D

24.某系统采用基于 IBC 技术的身份鉴别机制，需要搭建公开参数服务（PPS）供各方查询公开参数和标识状态信息。根据 GM/T 0057—2018《基于 IBC 技术的身份鉴别规范》，以下关于公开参数服务（PPS）的描述，正确的是哪一项？
A. PPS 仅用于发布 IBC 公开参数，不涉及用户标识信息
B. PPS 用于发布 IBC 公开参数、私钥生成策略、用户标识信息和状态等数据
C. PPS 仅用于查询用户标识状态，不涉及公开参数
D. PPS 由应用系统开发商自行定义，无需遵循标准规范
答案：B

25.某软件公司正在开发一款支持 PDF 文档密码应用的软件，需要明确该标准的适用范围，以确定其功能设计边界。根据 GM/T 0112—2021《PDF 格式文档的密码应用技术要求》，该标准规定了采用密码算法对 PDF 格式文档进行哪些操作

的技术要求？
A. 仅数字签名和电子签章
B. 仅加密和解密
C. 数字签名、电子签章以及加解密
D. 仅数字签名和加解密
答案：C

26.某单位开发 PDF 加密功能，需要确定 PDF 文档的加密方式。根据 GM/T 0112—2021《PDF 格式文档的密码应用技术要求》，该标准规定的 PDF 加解密机制包括以下哪几种方式？
A. 仅基于口令的加密
B. 仅基于数字证书的加密
C. 基于口令的加密和基于数字证书的加密
D. 仅基于对称密钥的加密
答案：C

27.某单位在 PDF 电子签章开发过程中，需要确定签章保护范围（ByteRange）的设置方式及签名算法的要求。根据 GM/T 0112—2021《PDF 格式文档的密码应用技术要求》，以下关于 PDF 电子签章 ByteRange 和签名算法要求的说法中，正确的有（ ）
A. ByteRange 范围包含电子签章值（Contents 条目）本身
B. ByteRange 范围是除电子签章值本身之外的整个文件
C. 对 PDF 文档的任何一个字节的变动都会造成签章验证失败
D. SM2 签名算法应遵循 GM/T 0003
答案：BC

28.根据 GM/T 0095—2020《电子招投标密码应用技术要求》，电子招投标系统中用于数据完整性校验与数字签名杂凑运算的国密算法是（）
A.SM1
B.SM2
C.SM3
D.SM4
答案：C

29.依据 GM/T 0095—2020《电子招投标密码应用技术要求》，电子招投标投标文件加密应优先采用的国密对称加密算法为（）
A.SM2
B.SM3
C.SM4
D.SM9
答案：C

30.GM/T 0095—2020《电子招投标密码应用技术要求》规定，电子招投标系统客户端身份认证与本地签名解密应使用的密码设备是（）
A.服务器密码机
B.智能密码钥匙

C.安全网关
D.密钥管理系统
答案：B

31.按照 GM/T 0095—2020《电子招投标密码应用技术要求》，电子招投标密码应用日志记录保存期限应不少于（）
A. 3 个月
B.6 个月
C.12 个月
D.24 个月
答案：B

32.根据 GM/T 0070—2019《电子保单密码应用技术要求》标准，电子保单投保环节中，保险业务系统客户端应采集签名者的手写签名笔迹信息、声音、影像等数据，形成投保行为证据链，并利用以下哪项完成电子投保申请的数字签名？（ ）
A. 保险公司的企业数字证书私钥
B. CA 颁发的投保人数字证书私钥
C. 保险代理人的注册账户数字证书
D. 时间戳服务机构的数字证书
答案：B

33.根据 GM/T 0070—2019《电子保单密码应用技术要求》标准，电子保单的签发环节中，电子保单系统应按照投保人填写的投保资料，根据险种的不同结合相应的保单内容模板，自动生成格式化保单数据，并进行以下哪项操作？（ ）
A. 在电子保单的投保人签章位置进行电子签章操作
B. 在电子保单的保险公司签章位置进行电子签章操作
C. 在电子保单的受益人签章位置进行电子签章操作
D. 在电子保单的所有页面进行电子签章操作
答案：B

34.根据 GM/T 0124—2022《安全隔离与信息交换产品密码检测规范》标准，安全隔离与信息交换产品的安全等级划分为哪两个级别？（ ）
A. 一级和二级
B. 基本级和增强级
C. 标准级和高级
D. A 级和 B 级
答案：B

35.根据 GM/T 0124—2022《安全隔离与信息交换产品密码检测规范》标准，安全隔离与信息交换产品定义中的核心特征是（ ）
A. 能够实现网络之间的高速数据交换
B. 能够在实现网络隔离的同时，通过网络协议终止基础上的安全通道进行安全数据交换
C. 仅能实现网络的物理隔离
D. 能够实现完全无限制的数据互通
答案：B

36.在区块链系统中，为了确保账本数据的不可篡改和前后链接，依据 GM/T 0111-2021《区块链密码应用技术要求》标准，在区块链账本中通常通过区块头的哪一项来识别区块并用于链接相邻区块？（ ）
A. 签名值
B. 权限值
C. 杂凑值
D. 时间戳
答案：C

37.依据 GM/T 0119-2022《PLC 控制系统及 PLC 控制器密码应用技术规范》标准，PLC 控制系统中各组成设备的密码应用需满足特定要求。其中，负责运行逻辑组态软件、实现用户逻辑组态编辑打包和下装的“工程师站”，在进行双向身份认证时主要采用的密码算法是？（ ）
A. SM4/SM3
B. SM2/SM9
C. SM3/SM4
D. SM2/SM4
答案：B

38.在数字证书格式符合性检测中，为了解决时间溢出问题并确保证书有效期编码的规范性，GM/T 0043-2024《数字证书互操作检测规范》对终端实体证书的有效期编码规则做出了明确要求。以下关于该编码规则的描述，正确的是？（ ）
A. 2049 年前采用 GeneralizedTime 类型，2050 年后采用 UTCTime 类型
B. 所有年份统一采用 UTCTime 类型
C. 2049 年前采用 UTCTime 类型，2050 年后必须使用 GeneralizedTime 类型
D. 所有年份统一采用 GeneralizedTime 类型
答案：C

39.依据 GM/T 0043-2024《数字证书互操作检测规范》，在进行数字证书互操作检测时，判定规则采用了“关键项一票否决”机制。对于提供 OCSP 服务的系统，其所有检测项的判定级别是如何规定的？（ ）
A. 仅包含关键项
B. 仅包含一般项
C. 关键项占 50%，一般项占 50%
D. 所有检测项均为关键项
答案：D

40.根据 GM/T 0106—2021《银行卡终端产品密码应用技术要求》，该标准主要规定了银行卡终端产品上密码应用相关的技术要求。以下哪项不属于该标准规定的内容？（ ）
A. 终端基本安全要求
B. 终端密钥管理要求
C. 终端数据安全要求
D. 终端硬件物理防破坏要求
答案：D

41.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

42.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

43.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

44.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

45.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

46.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

47.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

48.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

49.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

50.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

51.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

52.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

53.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

54.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

55.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

56.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

57.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

58.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

59.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

60.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

61.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

62.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

63.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

64.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

65.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

66.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

67.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

68.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

69.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

70.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

71.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

72.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

73.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

74.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

75.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

76.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

77.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

78.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

79.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

80.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

81.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

82.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 和 2
B.2 和 4
C.2 和 3
D.3 和 4
答案：D

83.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

84.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

85.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

86.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

87.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

88.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

89.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

90.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

二、多选题 125
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. 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

21. 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

22. 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

23. 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

24. 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

25. 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

26. 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

27. 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

28. 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

29. 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

30. 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

31. 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

32. 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

33. 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

34. 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

35. 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

36. 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

37. 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

38. 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

39. 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

40. 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

41. 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

42. 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

43. 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

44. 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

45. 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

46. 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

47. 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

48. 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

49. 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

50. 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

51. 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

52. 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.明文存储于数据库中
D.通过哈希算法处理后存储于数据库中
答案：AB

53. 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

54. 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

55. 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

56. 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

57. 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

58. 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

59. 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

60. 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

61. 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

62. 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

63. 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

64. 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

65. 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

66. 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

67. 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

68. 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

69. 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

70. 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

71. 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

72. 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

73. 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

74. 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

75. 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

76. 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

77. 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

78. 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

79. 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

80. 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

81. 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

82. 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

83. 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

84. 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

85. 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

86. 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

87. 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

88. 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

89. 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

90. 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

91. 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

92. 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

93. 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

94. 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

95. 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

96. 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

97. 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

98. 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

99. 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

100. 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

101. 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

102. 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

103. 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

104. 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.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.应将应急预案纳入密码应用岗位人员的培训和考核内容
答案：ABCD

105. 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

106. 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

107. 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

108. 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

109. 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

110. 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

111. 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

112. 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

113. 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

114. 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

115. 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

116. 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

117. 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

118. 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

119. 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

120. 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

121. 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

122. 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

123. 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

124. 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

125. 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 30
1. 根据 GM/T 0129-2023《SSH 密码协议规范》，在 SSH 连接协议的通道复用机制中，所有类型的通道（如会话通道、TCP/IP 转发通道等）均采用相同的通道号分配规则，且整个连接过程中通道号不得重复使用。
答案：错

2. GB/T 17964-2021《信息安全技术 分组密码算法的工作模式》中描述的所有工作模式都能同时保护数据的机密性和完整性。
答案：错

3. 在 CTR（计数器模式）中，加密和解密可以使用完全相同的运算结构，并且支持对任意顺序的分组进行加解密操作。
答案：对

4. 根据 GM/T 0021—2023《动态口令密码应用技术规范》，生成动态口令时，如果采用 SM4 算法，一次性中间值（OD）的输出长度应为 256 比特。
答案：错

5. 根据 GB/T 45654-2025《网络安全技术 生成式人工智能服务安全基本要求》，服务提供者应将模型训练环境与推理环境隔离，避免数据泄露、不当访问等安全事件。
答案：对

6. 根据 GB/T 43207—2023《信息安全技术 信息系统密码应用设计指南》，信息系统的密码应用方案只需按一个整体进行统一设计，无需按照责任主体划分不同部分。

答案：错

7. 根据 GB/T 43207—2023《信息安全技术 信息系统密码应用设计指南》，密码应用方案设计过程包括三项基本流程：密码应用需求分析、密码应用设计分析、安全与合规性分析。
答案：对

8. 根据 GB/T 17901.3-2021《信息技术 安全技术 密钥管理 第 3 部分：采用非对称技术的机制》，在密钥协商机制中，共享密钥由实体 A 单独选择并传递给实体 B，实体 B 无法预先确定该密钥值。
答案：错

9. 根据 GM/T 0074—2019《网上银行密码应用技术要求》，该标准仅适用于网上银行业务中密码技术相关安全功能的设计、实现和使用，手机银行系统不参照该标准。
答案：错

10. 根据 GM/T 0074—2019《网上银行密码应用技术要求》，在网上银行的数据机密性要求中，为保证数据内容机密性，仅需要对客户与网银系统间交互的登录信息和交易信息进行加密传输，而不包括签约信息和网银系统内存储的数据。
答案：错

11. 根据 GM/T 0108—2021《诱骗态 BB84 量子密钥分配产品技术规范》，该标准规定产品应具备日志管理功能。
答案：对

12. 根据 GM/T 0108—2021《诱骗态 BB84 量子密钥分配产品技术规范》，该标准基于采用弱相干态光源的诱骗态 BB84 协议，该协议的理论安全性已得到严格证明。
答案：对

13. 根据 GM/T 0032—2014《基于角色的授权管理与访问控制技术规范》，访问控制系统应在访问控制判定后完成身份鉴别。
答案：错

14. 根据 GM/T 0032—2014《基于角色的授权管理与访问控制技术规范》，属性管理系统可以采用属性证书系统或属性数据库等多种方式实现。
答案：对

15. 根据 GM/T 0057—2018《基于 IBC 技术的身份鉴别规范》，该标准规定的身份鉴别仅适用于基于 IBC 技术的双向身份鉴别场景，不涉及单向身份鉴别。
正确答案：错

16. 根据 GM/T 0112—2021《PDF 格式文档的密码应用技术要求》，该标准仅适用于 PDF 格式文档的数字签名和电子签章，不涉及加解密应用。
答案：错

17. 根据 GM/T 0112—2021《PDF 格式文档的密码应用技术要求》，在 PDF 电子签章的多重签章应用场景中，如果文档中已有电子签章，再进行签章处理时，应以覆盖原有签章的方式添加新签章。
答案：错

18. GM/T 0095—2020《电子招投标密码应用技术要求》规定，电子招投标全过程的电子签名与验证必须使用合法有效的数字证书，确保抗抵赖。（）
答案：对

19. 根据 GM/T 0070—2019《电子保单密码应用技术要求》标准，电子保单的存储安全管理中，应采用加密或其他保护措施实现鉴别信息存储的机密性，并采用适当的身份鉴别手段确保重要数据合法授权访问。
答案：对

20. 根据 GM/T 0070—2019《电子保单密码应用技术要求》标准，电子保单的数字签名与验证应采用国家密码管理主管部门批准的非对称密码算法 SM2 和杂凑算法 SM3，数据加密应采用 SM4 分组密码算法。
答案：对

21. 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

22. 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

23. 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

24. 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

25. 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

26. 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

27. 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

28. 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

29. 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

30. 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

$$
\begin{aligned}
&hint^{e} = m \bmod p \\
&hint^{e} - m = kp \\
&p = \gcd(hint^{e} - m, n)
\end{aligned}
$$

解题脚本

```
from Crypto.Util.number import *
import gmpy2

# 已知的参数
n                                                                                                   =
1223077692178488033976863493660743059462102609785227346789094927223043145544194
4020375049849543858159837867499207821927901278213214162837477927932356048352047
8724287077995018729807399806582903912854431760705676523361405189062684806859803
0880694876593597751369066167764435517704977017322693274986285726625326133924546
6179659463897520223155192412374696499405012791197307209479587540278975773758930
7583669780348544660566750431392494828727432169614332089975702900409231479986376
0418326579454342092056873088841972989722522584631832073250265026729065496071351
6982524877974781913378738339871260877641148498853785707733491123
hint                                                                                                =
1572627891288677364059712091776555284719743199383715535497290294794611273949217
9309176609759052666055364266668663243809191176807132013038131170302356498052356
7645585373349499905389148414618141628912491856704649508449912383247771843544095
5974249317038555427809388850125360469242105988300215702721170400802648658632210
3274281005193190863332679992913649924706180575798633407649278616217737494602327
6483306870981765168618097955933046034558585382525033251962256904180969504280123
```

```
65780913708070412151858679223925999860459480084953541318247343615442706782813734547625465432726661805609400089666596442168438455903612453438
ee =
56588769874868337589381845086515637235632440473433127609079491685276768954587549150447847272 9
ct =
11268613237540530679149877338155708929249800592798105860578249196281227290839486481891971836075094645380571208325084492787969416710430847707712103213938087179227063316505678745748633040919937440708490388710418074857599060108890036189432359871802475567613145060926547261450768168703467040088543396960510875557476776223203363977954176989285685842126761089114240490820415747103075106515843566365938690921933252267399125543250284309554597862406682250682657867484421876962715854938474211944019832267995782660091106417139453941849533833870672224453600227210469970714097243232696328126272622408389926314390923152087411592270

# 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

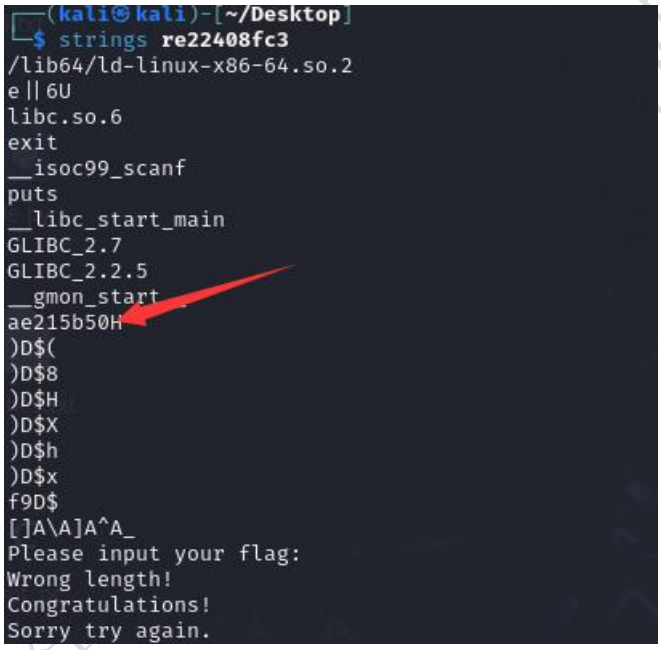
题干描述：

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：

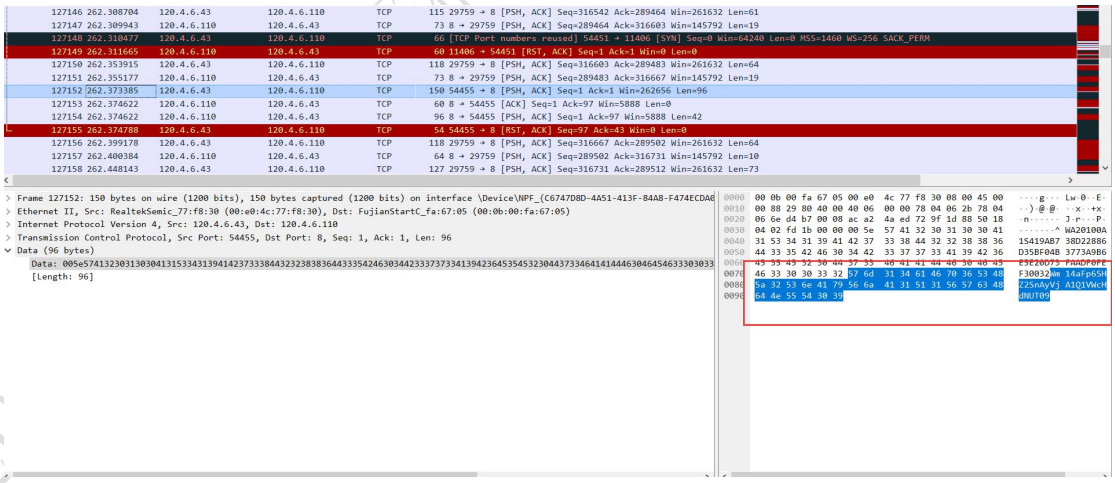
某金融云平台遭受了不明黑客组织攻击。经分析发现，异常流量是攻击者利用中间人攻击（MITM）技术，对银行金融密码机与核心系统之间的加密通信进行探测和截获。这台金融密码机负责执行关键的加密、解密和密钥管理操作，是银行处理大额交易和敏感金融信息的核心设备。攻击者成功捕获了密码机的一段流量包，并通过分析其中的通信数据，窃取操作员传输的敏感信息。为防止潜在的数据泄露和经济损失，银行迫切需要解密这些流量，识别并确认其中的有效字符。

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。

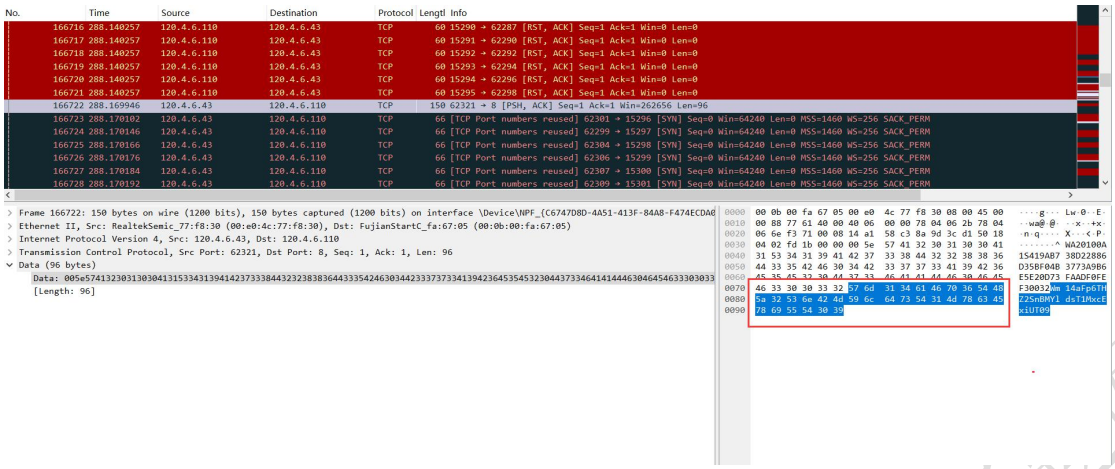
解题思路：

分析流量包，发现特殊的 4 段 hex 值 解码两次 base64

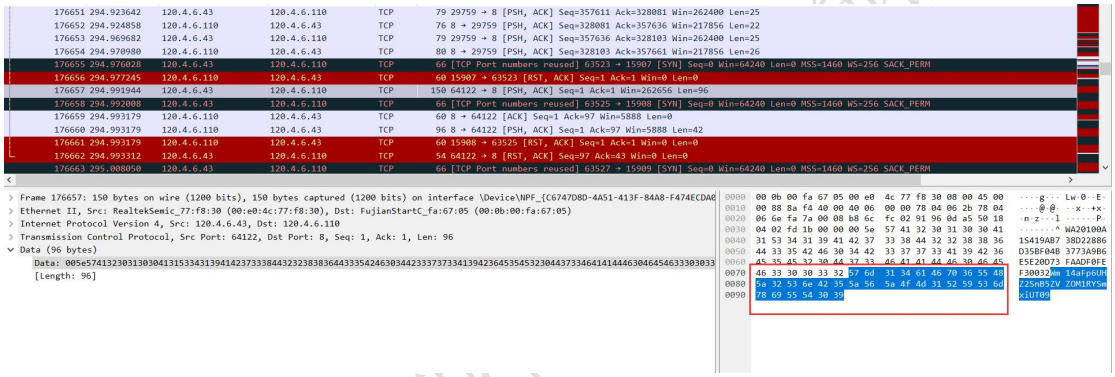
57 6D 31 34 61 46 70 36 53 48 5A 32 53 6E 41 79 56 6A 41 31 51 31 56 57 63 48 64 4E 55 54 30 39



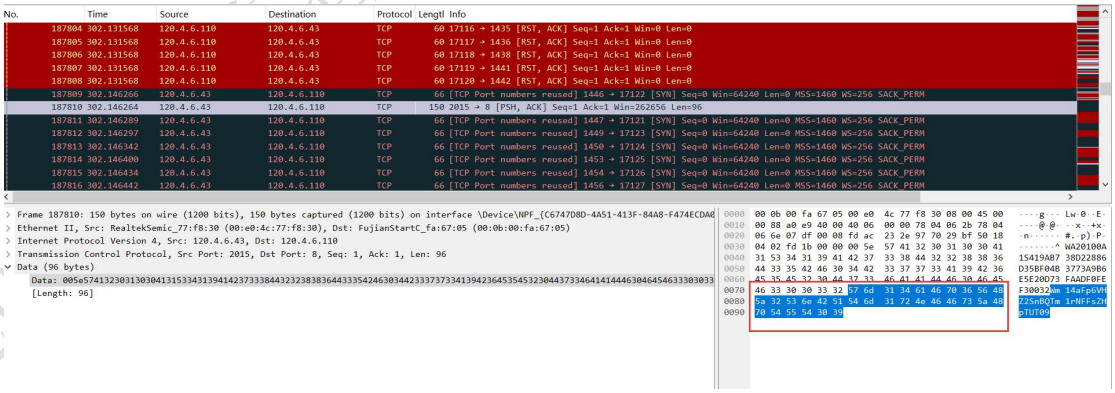
57 6D 31 34 61 46 70 36 54 48 5A 32 53 6E 42 4D 59 6C 64 73 54 31 4D 78 63 45 78 69 55 54 30 39

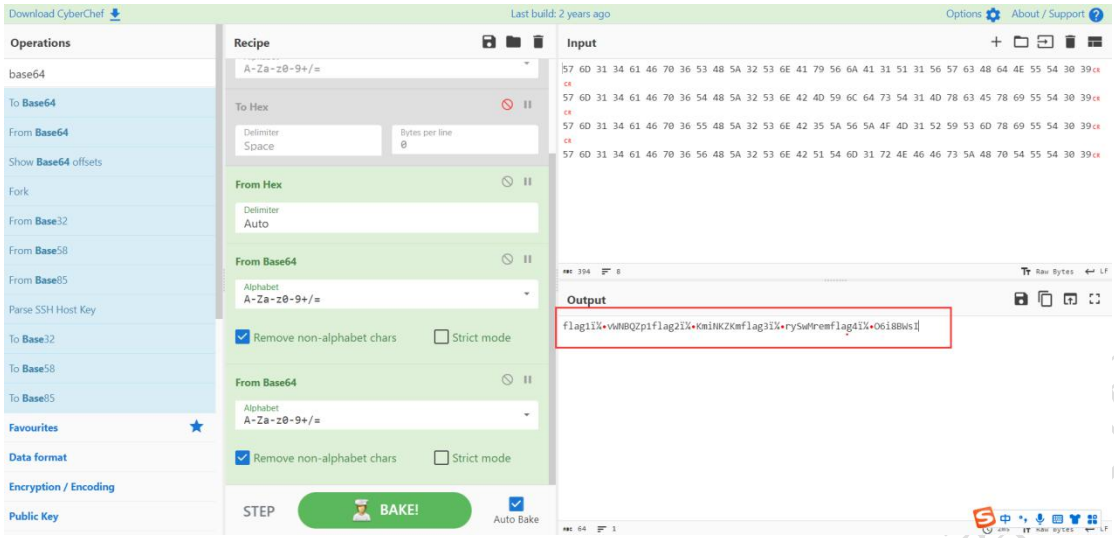


57 6D 31 34 61 46 70 36 55 48 5A 32 53 6E 42 35 5A 56 5A 4F 4D 31 52 59 53 6D 78 69 55 54 30 39



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

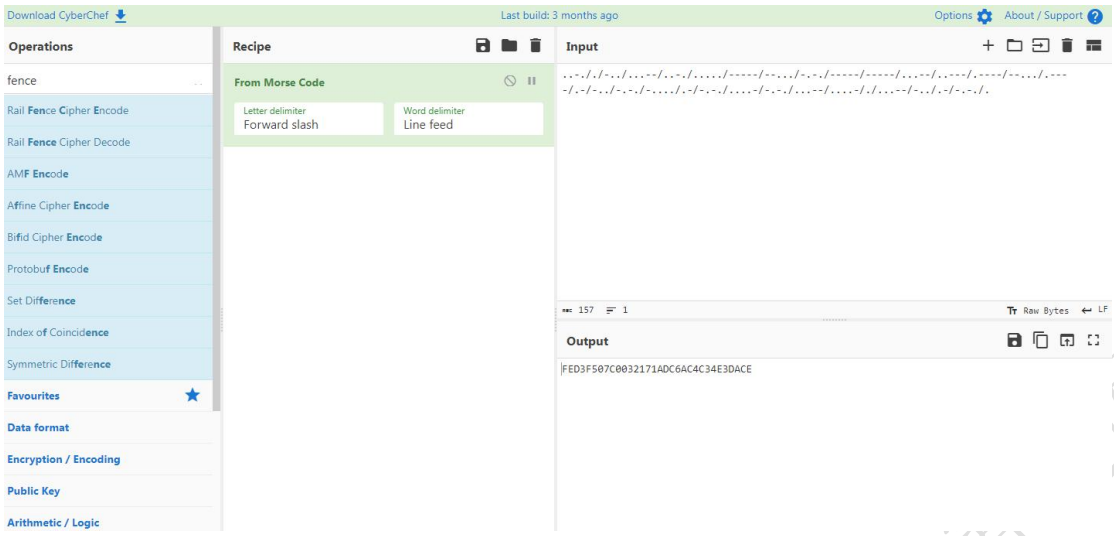
题干描述：

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}

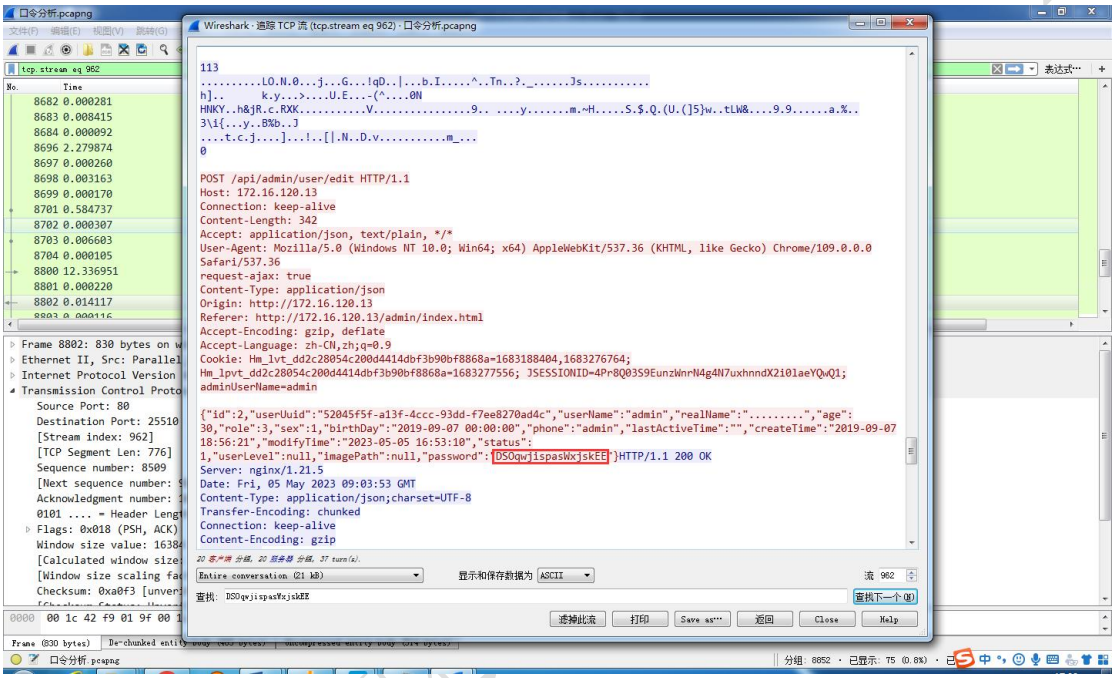
六、流量分析（analysis）

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：



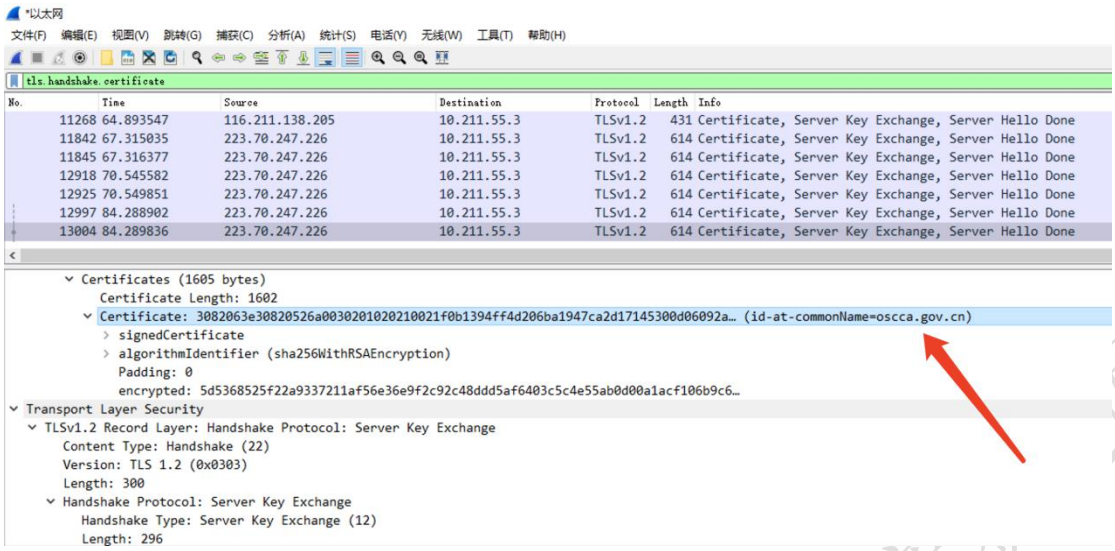
flag：flag{DSOqwjispasWxjskEE}

9、 oscca

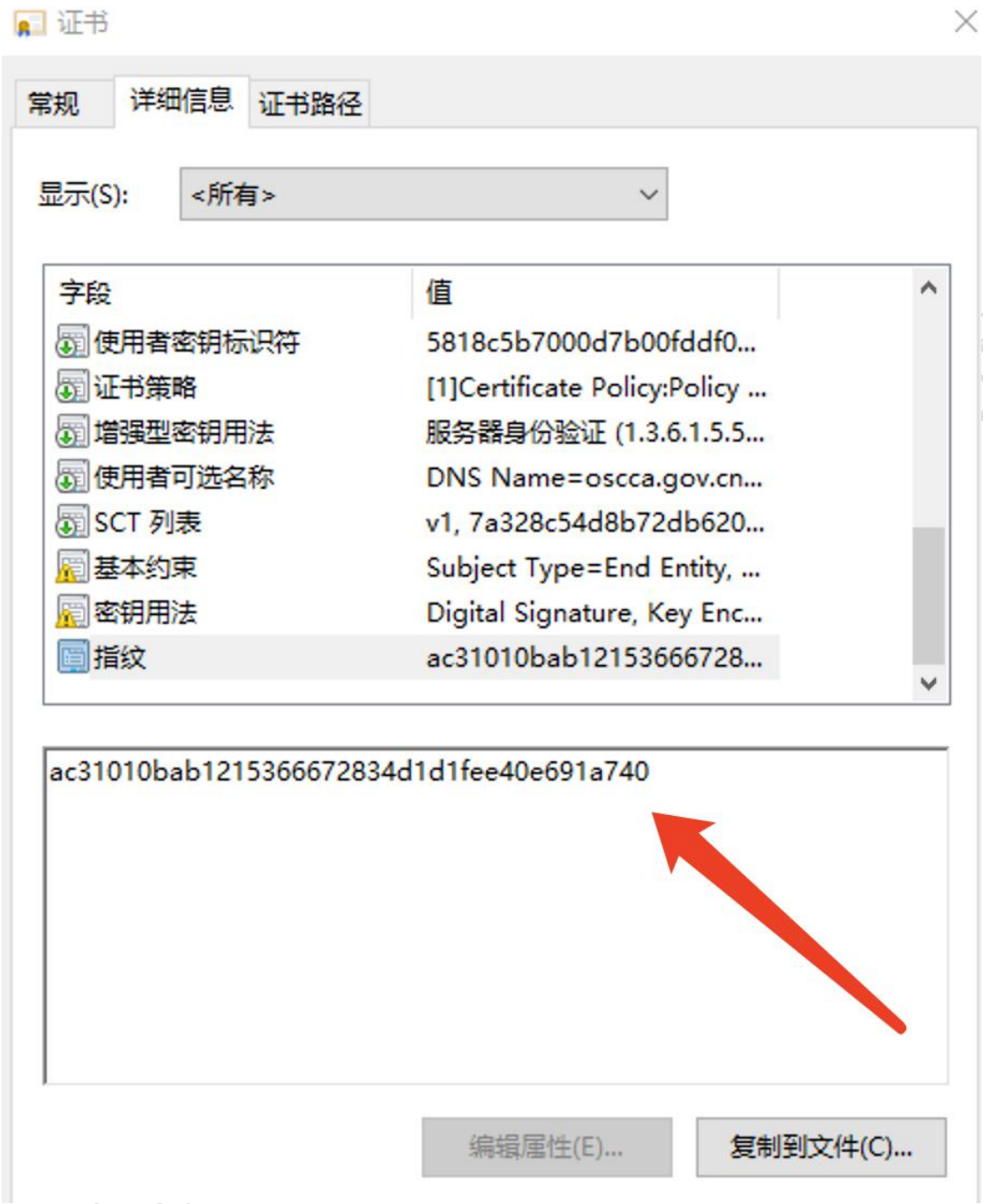
题干描述：

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

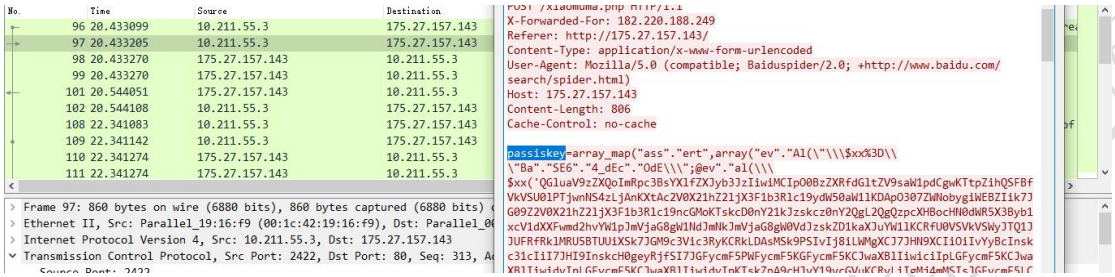
题干描述：

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

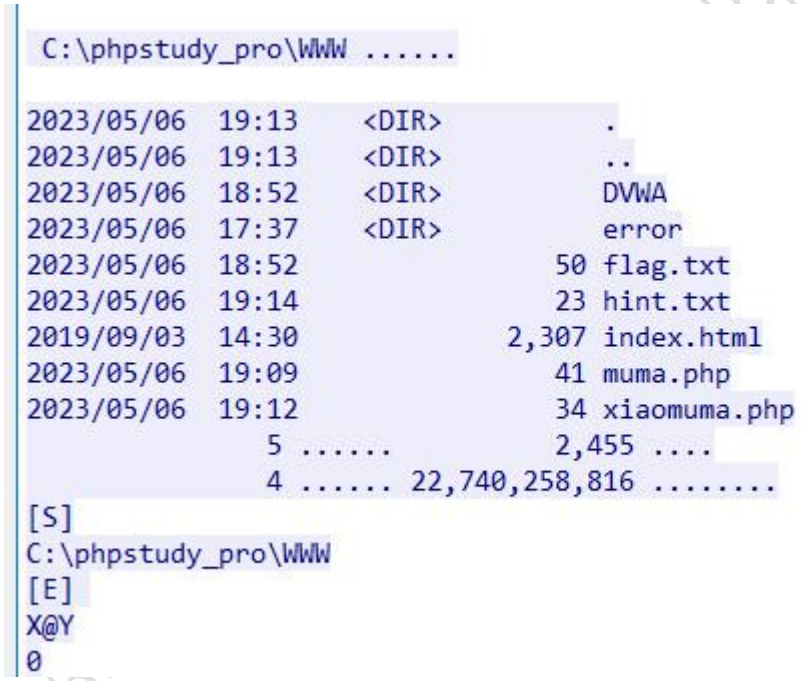
吗？

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

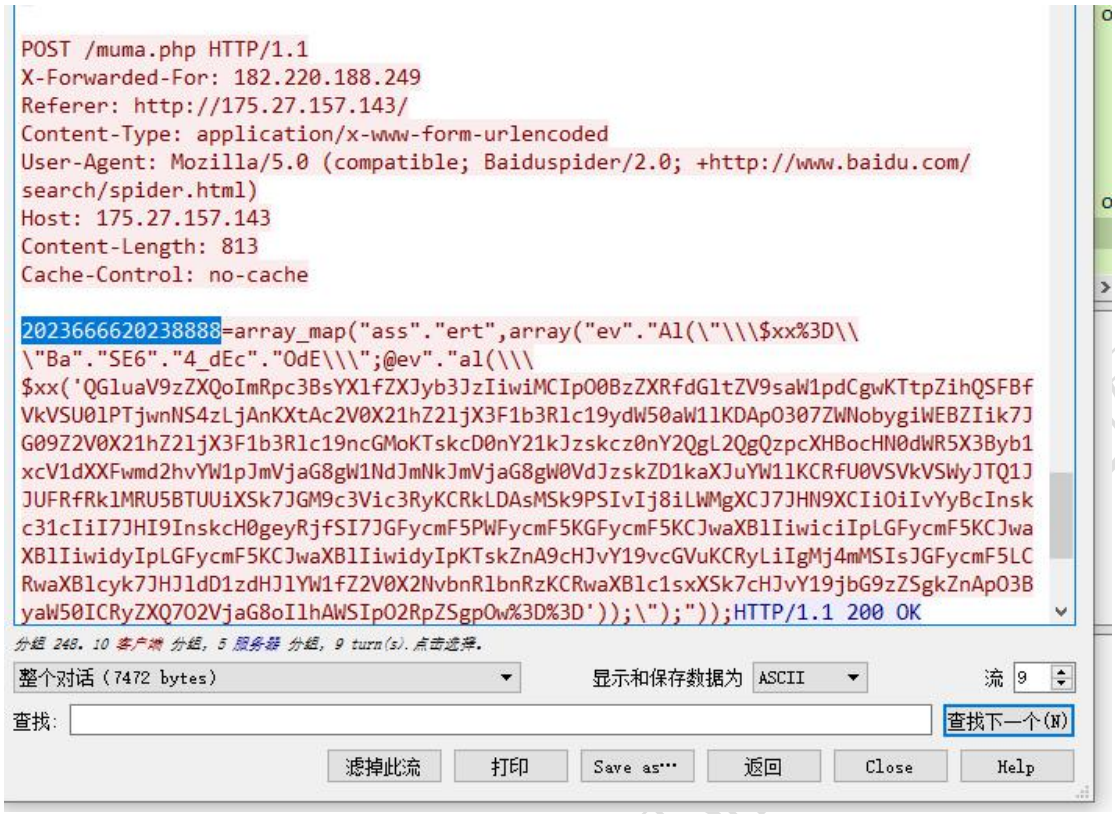
```
200 OK
Server: nginx/1.15.11
Date: Sat, 06 May 2023 11:15:31 GMT
Content-Type: text/html; charset=UTF-8
Transfer-Encoding: chunked
Connection: keep-alive
X-Powered-By: PHP/5.6.9

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}