企业管理 05

60 分钟内答卷

一、单选题（共 50 题，每题 1 分）

221.下面针对传递的不可否认性描述错误的是（） [单选题]*

A、产生证据的主体是接收者

B、不可以有第三方参与(正确答案)

C、证据验证者是发起者

D、证据信息至少包括接收者的身份和数据的精确值

222.通常在 SSL 协议中的哪次握手过程中判断采用何种密码套件（） [单选题]*

A、Client Hello

B、Server Hello(正确答案)

C、Server Key Exchange

D、Client Key Exchange

223.SSL 中在哪个协议中提供数据的保密性和完整性（） [单选题]*

A、握手协议

B、密码规格变更协议

C、报警协议

D、记录层协议(正确答案)

224.IPSec 在哪层协议中实现的通信双方身份鉴别（） [单选题]*

A、IKE 协议(正确答案)

B、AH 协议

C、ESP 协议

D、每个协议都有

225.下面有关 SM2 密钥交换协议描述错误的是（） [单选题]*

A、SM2 密码交换协议是 MQV 的一个变种

B、通讯双方经过一次信息传递，计算并获取会话密钥(正确答案)

C、协议中的每一个用户拥有一个公钥和私钥对

D、能提供认证性和前向安全性保障

226.下面关于 Diffie-Hellman 密钥交换协议描述错误的是（） [单选题]*

A、只能提供建立会话密钥的功能

B、不能抵抗中间人攻击

C、为每一个用户颁发一个公钥证书(正确答案)

D、不能提供互相认证的安全保障

227.下面针对我国的双证书体系描述错误的是（） [单选题]*

A、用户同时具有 2 个私钥，分别是签名私钥和加密私钥

B、签名私钥由用户在本地生成并专有掌握，对应证书为签名证书

C、加密私钥由专门的可信机构生成，用户不能掌握，对应证书为加密证书(正确答案)

D、加密私钥用于解密和密钥协商

228.数字证书中的签名值是对()的数字签名结果（） [单选题]*

A、整个证书

B、基本证书域(正确答案)

C、基本证书域和签名算法域

D、基本证书域、签名算法域和签名值域

229.数字证书中的签名结果值是（）类型 [单选题]*

A、OCTET STRING

B、BIT STRING(正确答案)

C、SET

D、SEQUENCE

230.按照我国标准，数字证书中 SM2 的签名算法标志符为（） [单选题]*

A、 1.2.156.10197.1.301(正确答案)

B、 1.2.156.10197.1.302

C、 1.2.156.10197.1.303

D、 1.2.156.10197.1.304

231.下面哪个不属于 PKI 系统组件（） [单选题]*

A、证书认证中心、注册机构、密钥分发系统(正确答案)

B、证书持有者、依赖方

C、证书撤销列表、资料库

D、轻量目录访问协议、在线证书状态协议

232.在点到点的密钥分发结构中，如果有 n 个成员组成的团队希望互相通信，那么需要人工分发的密钥加密密钥(KEK)的数量为(C) *

A、n(正确答案)

B、n2

C、 n(n-1)/2

D、 n!

233.下面针对密钥归档和密钥销毁描述错误的是（） [单选题]*

A、密钥在其生命周期结束时，应当进行销毁；

B、签名密钥对的私钥必须进行归档；(正确答案)

C、密钥归档是在密钥销毁后对密钥进行保存；

D、密钥进行销毁时，应当删除所有密钥副本，但不包括归档的密钥副本。

234.下面针对密钥使用的说法错误的是（） [单选题]*

A、用于核准的密码算法的密钥，不能再被非核准的密码算法使用；

B、不同类型的密钥不能混用；

C、需要保护公钥的保密性；(正确答案)

D、公钥在使用前需要验证公钥的完整性，以及与实体的关联关系。

235.下面针对密钥的导入和导出描述错误的是（） [单选题]*

A、密钥可以在同一个密码产品进行导入和导出，也可以从一个密码产品导出后再倒入另一个密码产品；

B、安全的密钥导入和导出方式包括加密传输和知识拆分；

C、SM4 的密钥导出，可以使用知识拆分成 2 个 64 比特的密钥分量进行导出；(正确答案)

D、高安全等级的密码产品还要求进行支持拆分后的密钥分量要通过可信信道传输。

236.下面针对密钥生成的描述错误的是（） [单选题]*

A、密钥生成的方式包括随机数直接生成和通过密钥派生函数(KDF)生成；

B、使用口令生成密钥时，密钥可以不在密码产品内部产生；(正确答案)

C、8 位数字口令仅提供 227 的密钥空间；

D、KDF 生成的密钥分为：从共享秘密派生密钥和从主密钥派生密钥。

237.下面对杂凑算法的描述错误的是（） [单选题]*

A、MD5 算法最终输出 128 比特的信息摘要，SHA-1 消息摘要长度为 160 比特；

B、SHA-2 算法支持 224、256、384 和 512 比特四种长度的输出；

C、SHA-3 算法支持 224、256、384 和 512 比特四种长度的输出；

D、通常所说的 SHA-256、SHA-512，指得是 SHA3 算法。(正确答案)

238.下面针对 HMAC 的描述错误的是（） [单选题]*

A、利用杂凑算法，将一个密钥和一个消息作为输入，生成一个消息摘要作为输出；

B、可用作数据完整性检验

C、可用作消息鉴别，保证信息源的真实性

D、SM3 的 HMAC 的密钥长度为 k，k=256(正确答案)

239.下面针对 SM3 算法描述错误的是（） [单选题]*

A、SM3 生成 256 比特的杂凑值；

B、SM3 的填充分组为 512 比特长

C、SM3 压缩函数输入由 512 比特的输入信息分组和上一次迭代过程的 512 比特输出组成；(正确答案)

D、SM3 算法的综合性能指标与 SHA-256 的同等条件下相当。

240.下面针对杂凑算法的 M-D 模型描述错误的是（） [单选题]*

A、SM3 和 SHA-3 算法采用的是 M-D 模型；(正确答案)

B、很长的消息经过 M-D 的压缩函数都会输出固定比特长度的数据；

C、如果压缩函数具有抗碰撞能力，那么杂凑算法也具有抗碰撞能力；

D、杂凑算法具有抗碰撞能力，压缩函数不一定有抗碰撞能力。

241.下面针对 RSA 算法描述错误的是（） [单选题]*

A、加密计算速度要比解密计算速度快很多倍；

B、生成的公钥中 2‰的不是按随机理论产生的，存在安全隐患；

C、RSA 算法基于大整数因子分解问题的困难性设计的；

D、RSA-1024 中的 1024 是指(正确答案)

e 的长度。

242.下面针对 SM9 描述错误的是（） [单选题]*

A、SM9 密码算法使用 256 比特的 BN 曲线

B、SM9 密码算法应用于管理需要数字证书；(正确答案)

C、签名者持有的私钥由密钥生成中心通过主私钥和签名者标识结合产生；

D、验证者用签名者的标识生成其公钥，验证签名的可靠性。

243.下面针对 SM2 描述错误的是（） [单选题]*

A、SM2 算法的推荐参数是定义在 256 比特素域上的

B、SM2 算法使用的私钥长度为 256 比特；

C、SM2 算法的公钥长度为 256 比特；(正确答案)

D、SM2 产生的密文比明文长 768 比特

244.下面对数字签名算法描述错误的是（） [单选题]*

A、数字签名一般需要先使用杂凑算法对原始信息进行杂凑运算；

B、数字签名使用公钥对信息进行签名，用私钥对签名数据进行检验；(正确答案)

C、数字签名可用于确认数据的完整性；

D、数字签名可用于确认签名者身份的真实性。

245.AES-256 的分组长度是（） [单选题]*

A、16 字节(正确答案)

B、32 字节

C、64 字节

D、128 字节

246.下面针对 SM4 算法的描述错误的是（） [单选题]*

A、数据分组长度为 128 比特，密钥长度 128 比特；

B、在设计上实现了资源重用，密钥扩展过程和加密过程类似；

C、加密过程与解密过程相同；

D、非常适合 64 位处理器实现(正确答案)

248.下面针对 CTR 分组模式特点描述错误的是（） [单选题]*

A、具有流密码预先生成密钥流的特征；

B、只用到了分组密码算法的分组加密操作；

C、错误密文中的对应比特质会影响解密后明文中对应比特；

D、输入明文信息必须是分组长度的整数倍。(正确答案)

249.下面针对 ECB 模式特点描述错误的是（） [单选题]*

A、对某一个分组的机密或者解密非独立于其他分组进行；(正确答案)

B、对密文分组的重排将导致明文分组的重排；

C、相同的明文分组会产生相同的密文分组；

D、不能抵抗分组的重放、嵌入和删除攻击。

企业管理 05

一、单选题（共 50 题，每题 1 分）

250.下面针对 CBC 模式的加密算法中 IV 初始向量描述正确的是（） [单选题]*

A、IV 需要保密

B、收发双方必须选用同一个 IV(正确答案)

C、IV 用于每次分组计算

D、加密过程中用的 IV 为固定值

251.下面哪些不是序列密码算法（） [单选题]*

A、ZUC

B、SM4(正确答案)

C、SNOW

D、RC4

252.下面针对轻量级密码算法描述错误的是（） [单选题]*

A、轻量级对称密码算法是指适用于计算能力、能力供应、存储空间和通信带宽等资源受限的设备的对称密码算法；

B、PRINCE、SIMON 等为轻量级分组密码算法；

C、格密码可用于设计轻量级对称密码算法；(正确答案)

D、轻量级密码算法并没有替代传统密码算法的趋势。

253.下面对密文同态操作错误的是（） [单选题]*

A、基于思想格上的困难问题设计的同态加密算法仅支持乘法同态操作(正确答案)

B、可以在密文状态下对数据进行计算和处理

C、支持密文状态的检索操作

D、需要做到全同态操作

254.密钥攻击的手段有哪些说法是不正确的（） [单选题]*

A、通过侧信道攻击获取私钥和随机数等信息

B、通过后门攻击获取私钥和随机数等信息

C、通过分析二进制代码提取密钥

D、通过白盒攻击将分离提取出密码混淆技术的密钥(正确答案)

255. 2012年，NIST 宣布()算法成为新的杂凑算法标准（） [单选题]*

A、MD5

B、SHA-1

C、SHA-2

D、Keccak(正确答案)

256.RSA 算法设计基于的数学难题是（） [单选题]*

A、椭圆曲线的离散对数问题；

B、最坏情况下的格上困难问题；

C、普通的离散对数问题；

D、大整数因子分解问题(正确答案)

257.香浓关于保密通信理论的发表和美国数据加密标准()的公布，以及公钥密码思想的提出，标志着现代密码时期的开启和发展。（） [单选题]*

A、AES

B、RSA

C、DES(正确答案)

、MD

258.评价密码系统的五条标准有：（）、加密操作的复杂性、误差传播和信息扩展。 [单选题]*

A、保密度、密钥量(正确答案)

B、机密性、密钥量

C、机密性、加密强度

D、保密度、加密强度

259.机械密码的典型代表恩尼格玛密码机使用的是什么密码系统：（） [单选题]*

A、单表代换密码系统

B、多表代换密码系统(正确答案)

C、置换密码系统

D、多置换密码系统

260.戴明环管理循环，是一种经典的信息安全过程管理方式，它的过程是 计划-实施-（）-改进”。 [单选题]*

A、检测

B、评估

C、检查(正确答案)

D、验证

261.密码是指使用特定变换的方法对（）等进行加密保护、安全认证的技术、产品和服务。 [单选题]*

A、数据

、信息(正确答案)

C、文件

D、内容

262.L 密码应用方案设计是信息系统密码应用的起点，它直接决定这信息系统的密码应用是否合规、正确、有效地部署实施。以下是密码应用方案设计原则（） [单选题]*

A、总体性原则、科学性原则

B、总体性原则、完备性原则、可行性原则

C、总体性原则、科学性原则、可行性原则

D、总体性原则、科学性原则、完备性原则、可行性原则(正确答案)

263.L 数字证书认证系统是对生命周期内的数字证书进行全过程管理的安全系统，属于数字证书认证系统密码检测类标准的是（） [单选题]*

A、 GM/T0037-2014(正确答案)

B、 GM/T0020-2012

C、 GM/T0015-2012

D、 GM/T0014-2012

264.L 签名验签服务器是为应用实体提供基于 PKI 体系和数字证书的数字签名、验证签名等运算功能的服务器，可以保证关键业务信息的真实性、完整性和不可否认性，签名验签服务器可以通过那些方式提供服务（） [单选题]*

A、API 调用方式

B、请求响应方式

C、WEB 方式

D、以上说法都正确(正确答案)

265.L IPSecVPN 和 SSLVPN 两者工作不同的网络层次搭建通道，IPSecVPN 是在哪一层进行工作（） [单选题]*

A、网络层(正确答案)

B、应用层

C、会话层

D、传输层

266.L 对密码应用合规性、正确性、有效性的检测评估，检测与评估的关系描述错误的是（） [单选题]*

A、检测是定性，评估是定量(正确答案)

B、检测是现实结果，评估是预测未来

C、检测是客观的，评估有主观性

D、检测关注具体，评估强度综合

267.L 以下专业术语描述错误的是（） [单选题]*

A、线性分析(linear cryptanalysis)

B、中间人攻击(man-in-the-middle attack)

C、全同态加密(fully homomorphic encryption)

D、真实性(authenticit)(正确答案)

268.L 下面关于《中华人民共和国密码法》描述错误的是（） [单选题]*

A、国家推进商用密码检测认证体系的建设，制定商用密码检测认证技术规范、规则，商用密码从业单位须接受商用密码检测认证，提升市场竞争力。(正确答案)

B、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机构进行认定，会同有关部门负责政务活动中使用电子签名、数据电文的管理。

C、商用密码领域的行业协会等组织依照法律、行政法规及其章程的规定，为商用密码从业单位提供信息、技术、培训等服务，引导和督促商用密码从业单位依法开