

## 《现代密码学》参考例题

### 一、单选

1. 加密和解密都是在\_\_\_\_\_控制下进行的  
A. 口令      **B. 密钥**      C. 字符串      D. 算法
2. 恺撒密码属于\_\_\_\_\_体制  
A. 置换密码      **B. 移位密码**      C. 转轮机密码      D. 以上都不对
3. 下列哪个不是分组密码体制\_\_\_\_\_  
A. DES    B. AES    C. IDEA      **D. RC4**
4. CBC 模式中, 一个密文分组传输错误, 会影响\_\_\_\_\_个密文分组的解密  
A. 1      **B. 2**      C. 3      D. 4
5. 1976 年, 提出公钥密码系统的学者是 \_\_\_\_\_  
A. Miller、Rabin      B. Bellare、Rogway  
C. Adelman、Shamir      **D. Diffie、Hellman**
6. 略
7. 为加快计算速度, RSA 中 e 一般不取哪个值\_\_\_\_\_  
A. 3      B. 17      **C. 32767**      D. 65537
8. 下列哪个是公钥证书格式的标准\_\_\_\_\_  
A. X.500      **B. X.509**      C. LDAP      D. OCSP
9. 哪个不属于信息安全的三要素\_\_\_\_\_  
A. 机密性      **B. 非否认**      C. 完整性      D. 可用性
10. 弗吉尼亚密码属于\_\_\_\_\_体制  
A. 置换密码      **B. 多表代换密码**      C. 转轮机密码      D. 以上都不对
11. \_\_\_\_\_不是分组密码的工作模式  
A. CBC      B. OFB      C. CTR      **D. MAC**
12. 非奇异椭圆曲线上的点集与哪个运算构成群\_\_\_\_\_  
**A. 加法**      B. 减法      C. 乘法      D. 除法
13. 流密码体制由\_\_\_\_\_两部分组成  
A. 驱动部分、反馈函数      B. FSR、反馈函数  
C. FSR、非线性组合部分      **D. 驱动部分、非线性组合部分**
14. 设计分组密码的两种技术是\_\_\_\_\_  
A. 置换和移位      **B. 混乱和扩散**  
C. 易位和置换      D. 隐写和扩散
15. 按照攻击者知道信息的多少, 哪个不属于密码分析的类别  
A. 唯密文攻击    B. 已知明文攻击    C. 选择明文攻击      **D. 虫洞攻击**
16. RSA 的安全性基于\_\_\_\_\_困难假设  
A. 离散对数问题      B. 背包问题  
**C. 大整数分解问题**      D. Diffie-Hellman 问题
17. 数字签名无法提供的特性是\_\_\_\_\_  
A. 抗伪造      B. 非否认      **C. 保证可用性**      D. 不可重用性  
PS: 不可重用性是指一个数字签名只与一条消息相关联, 把为某条消息产生的数字签名用到其他消息上是不行的, 也即数字签名和消息之间是相互绑定的关系。
18. 关于公钥密码与对称密码相比较, 下列哪个说法不正确\_\_\_\_\_  
A. 公钥密码密钥较长      **B. 公钥密码更安全**

- C. 公钥密码应用历史短 D. 公钥分发比较复杂
19. 提出基于身份密码学的学者是\_\_\_\_\_
- A. Shamir B. Diffie C. Hellman D. Rogaway
20. MAC 算法的功能是实现数据的\_\_\_\_\_
- A. 机密性 B. 完整性 C. 可用性 D. 非否认
21. 哪个不属于单表代换密码\_\_\_\_\_
- A. 凯撒密码 B. 移位密码 C. 弗吉尼亚密码 D. 以上答案都不对
22. 转轮机密码属于\_\_\_\_\_
- A. 古典密码 B. 公钥密码 C. 密钥交换协议 D. 秘密共享
23. 下列哪个不属于公钥密码体制的范畴\_\_\_\_\_
- A. RSA B. ElGamal C. DES D. ECC
24. 哪个学者没有参与提出 RSA\_\_\_\_\_
- A. Shamir B. Hellman C. Rivest D. Adleman
25. 下列哪个不是对称密码体制的缺陷\_\_\_\_\_
- A. 密钥管理困难 B. 计算速度慢 C. 无法实现“非否认” D. 存在密钥分发问题
26. 扩展的欧几里得算法可用于计算\_\_\_\_\_
- A. 模运算下的求幂 B. 逆元 C. 最小公倍数 D. 离散对数
27. 哪门学科告诉我们世界存在真正的随机性\_\_\_\_\_
- A. 量子力学 B. 密码学 C. 混沌学 D. 天体物理
28. 在椭圆曲线中, 求点  $P+P$  时, 几何作图需要\_\_\_\_\_
- A. 对  $P$  点做切线 B. 连接点  $P$  和点  $O$  C. 连接  $P$  点和原点 D. 以上都不对
29. 视觉密码的提出者是\_\_\_\_\_
- A. Shamir B. Hellman C. Adleman D. Rivest
30. 制约基于身份密码学发展的主要桎梏是\_\_\_\_\_
- A. 私钥丢失了怎么办 B. 不太安全 C. 应用背景不明确 D. 以上答案都不对
31. 密码学的组成包括密码编码学和\_\_\_\_\_
- A. 密码设计学 B. 密码破译学 C. 密码分析学 D. 以上答案都不对
32. CA 的主要任务是\_\_\_\_\_
- A. 签发和管理证书 B. 检验证书申请者身份  
C. 作废过期证书 D. 以上都不对
33. 下列哪个不是 RSA 的缺点\_\_\_\_\_
- A. 无法证明对 RSA 的破译是否等同于大整数分解问题  
B. 计算速度相对较慢  
C. 只能用于加密, 不能用于签名  
D. 选择合适的  $p$ 、 $q$  对于普通用户来说比较困难
34. 多表代换密码中, 采用字母为密钥, 且密钥长度是  $m$ , 密钥空间大小为\_\_\_\_\_
- A.  $(26^m)!$  B.  $26^m$  C.  $m!$  D.  $m^{26}$
35. 双线性映射是属于\_\_\_\_\_范畴的技术
- A. 分组密码 B. 流密码 C. 椭圆曲线密码 D. 以上答案都不对
36. 双线性映射技术应用于\_\_\_\_\_椭圆曲线
- A. 非奇异 B. 奇异 C. 超奇异 D. 任何
37. RSA 中, 哪个不是在选择  $p$  和  $q$  时需要注意的问题\_\_\_\_\_
- A.  $p$ 、 $q$  不能相同, 同时既不要太接近, 又不能差别太大  
B.  $p$ 、 $q$  是安全素数

- C.  $\gcd(p-1, q-1)$  应当小
- D.  $p-1$ 、 $q-1$  不能有公因子**
38. 下面哪种说法不正确\_\_\_\_\_
- A. 密码学由密码编码学、密码分析学两部分组成
- B. 密码编码学主要关注如何设计密码
- C. 密码分析学主要关注如何破译密码
- D. 密码分析学对密码设计没有任何促进作用**
39. 周期置换密码中, 明文分组长度是  $m$ , 密钥空间大小为\_\_\_\_\_
- A.  $m!$**       B.  $2^m$       C.  $m$       D.  $m^2$
40. 对文件加密时, 最好选用哪种模式\_\_\_\_\_
- A. ECB    **B. CBC**    C. OFB    D. CFB
41. 下面哪个说法不正确的\_\_\_\_\_
- A. 对 Hash 函数的攻击就是寻找一对碰撞的过程
- B. 迭代构造 Hash 函数时, 预处理过程必须是单射的
- C. 对 Hash 函数的生日攻击说明, 输出长度与其安全性无关**
- D. Hash 函数具有压缩功能
42. 下面哪个的提出与 Shamir 无关\_\_\_\_\_
- A. MD5**    B. IBC    C. RSA    D. 视觉密码
43. 密码学中的 CATCH-22 问题是指\_\_\_\_\_
- A. 对称密码存在密钥爆炸的问题      B. 对称密码无法实现非否认
- C. 无法证明共享密钥的秘密通信是否是安全的**      D. 无法证明 P 与 NP 是否相等
44. 一般伪随机序列具有的特性是\_\_\_\_\_
- A. 不能可靠获得      B. 具有不可预测性      **C. 看上去是随机的**      D. 以上都对
45. 不属于双线性映射特性的是\_\_\_\_\_
- A. 双线性    B. 非退化性    C. 可计算性    **D. 差分性**
46. 与传统公钥密码相比, ECC 的优点是\_\_\_\_\_
- A. 安全性高    B. 灵活性好    C. 密钥长度更短    **D. 以上都对**
47. IBC 中的密钥托管问题是指\_\_\_\_\_
- A. ID 如果发生泄露, 其安全性会受到威胁
- B. 私钥泄露以后, 相应的 ID 也就无法使用
- C. 一旦 TA 被攻破, 所有用户信息将受到威胁**
- D. 以上都不对
48.  $(E, +)$  的单位元通常用\_\_\_\_\_表示
- A. O**      B. P      C. Q      D. R
49. 下面哪个属于真正的单向函数\_\_\_\_\_
- A. 离散对数    B. 背包    C. 大整数分解    **D. 以上答案都不对**
50. P 与 NP 之间的关系是\_\_\_\_\_
- A.  $P=NP$       B.  $P \neq NP$       C.  $P \cap NP = \Phi$       **D. 关系未确定**
51. 身份认证技术可以用于防范哪种攻击\_\_\_\_\_
- A. 窃听    **B. 冒充**    C. 社会工程学    D. 篡改
52. 以下说法正确的是\_\_\_\_\_
- A. 维吉尼亚密码不能用手工破译
- B. 一次一密可以达到绝对安全性
- C. 密钥空间大并不意味着密码体制就是安全的**

- D. Enigma 是一种复杂的置换密码体制
53. CTR 模式中, 一个密文分组传输错误, 会影响\_\_\_\_\_个密文分组的解密  
A. 2      **B. 1**      C. 4      D. 3
54. 最早发明频率分析的是\_\_\_\_\_  
A. 德国人      B. 英国人      **C. 阿拉伯人**      D. 美国人
55. IBC 中 TA 的主要任务是\_\_\_\_\_  
**A. 产生用户私钥**      B. 检验申请者身份      C. 签发证书      D. 以上都不对
56. 目前, RSA 的模数  $n$  至少是\_\_\_\_\_比特, 才能达到安全要求  
A. 512      B. 3096      C. 2048      **D. 1024**
57. 双线性映射技术可以\_\_\_\_\_  
**A. 将曲线上两个点映射到其基域的一个元素**  
B. 将曲线上一个点映射到其基域的一个元素  
C. 将基域的一个元素映射到曲线上的一个点  
D. 以上都不对
58. 洛伦茨密码属于\_\_\_\_\_  
**A. 转轮机**      B. 移位密码      C. 单表代换密码      D. 现代密码体制
59. 消息认证技术可以用于防范哪种攻击\_\_\_\_\_  
A. 窃听      **B. 篡改**      C. 社会工程学      D. 泄露
60. 移位密码的密钥空间大小是\_\_\_\_\_  
**A. 26**      B.  $26!$       C.  $26^m$       D. 以上答案都不对
61. RC4 属于\_\_\_\_\_  
A. 分组密码      B. 公钥密码      **C. 流密码**      D. 古典密码
62. 以下说法正确的是\_\_\_\_\_  
A. 网络安全为密码学提供理论和技术支持  
B. 一次一密可以证明能达到绝对安全性  
**C. 有些安全需求无法用密码学实现**  
D. Enigma 是一种复杂的置换密码体制
63. 下面说法正确的是\_\_\_\_\_  
**A. 口令机制是进行身份认证最简单、最常用的机制**  
B. Java 环是一种密码加速器  
C. 用对称密码加密时, 如果明文长度正好是明文分组长度的整数倍, 则无需填充  
D. 为抵抗在线攻击, 口令不能以明文形式保存
64. 对称加密体制包括\_\_\_\_\_  
**A. 序列密码、分组密码**      B. 序列密码、ECC      C. 分组密码、RSA      D. 以上都不对
65. 为什么不直接使用种子作随机数\_\_\_\_\_  
A. 随机数必须随机产生      B. 种子易被猜测      **C. 种子的熵太低**      D. 以上都不对
66. Diffie 和 Hellman 提出公钥思想时, 主要解决了以下哪个问题\_\_\_\_\_  
A. 设计公钥加密体制      **B. 从未见过面的两个人如何实现秘密通信**  
C. 如何提高加密体制的安全性      D. 提出了 ECC
67. 数字签名至少要满足的两个条件是\_\_\_\_\_  
A. 可验证性、可用性      B. 不可伪造性、可用性  
**C. 可验证性、不可伪造性**      D. 以上都不对
68. 为什么要提出基于身份的密码学\_\_\_\_\_  
**A. 避免使用复杂的 PKI 系统**      B. 使密码系统更安全

- C. 加快算法速度    D. 以上都不对
69. 以下哪个事件说明在使用伪随机序列发生器时选择“好”的种子很重要\_\_\_\_\_
- A. Shamir 发明了差分密码分析    B. “9.11”事件  
**C. I. Goldberg 和 D. Wagner 攻击 SSL**    D. OpenSSL 的“心脏出血”攻击
70. “任何人考虑用数学的方法产生随机数肯定是不合理的”这句话是谁说的\_\_\_\_\_
- A. Hellman    B. Shamir    **C. von Neumann**    D. Diffie
71. 密码学的研究内容主要是指\_\_\_\_\_
- A. 保护系统安全**    B. 设计密码体制    C. 破译密码体制    D. 以上都不对
72. 根据 CATCH-22 问题, 对称密码体制中, 密钥\_\_\_\_\_
- A. 可以通过公开信道传递    **B. 需要通过秘密信道传递**  
 C. 无需传递就可以进行通信    D. 以上都不对
73. 下面关于 PBE, 说法正确的是\_\_\_\_\_
- A. 用户只需记住口令, 而无需记住密钥**    B. 从口令直接推导出密钥  
 C. salt 必须加密    D. 引入 salt 的目的是为了增强安全性
74. 下面关于 CTR 模式, 说法不正确的是\_\_\_\_\_
- A. 有限差错传播**    B. 适用于并行加密    C. 可以随机访问    D. 可证明安全性
75. KEK 的作用是什么\_\_\_\_\_
- A. 它是整个系统的主密钥    **B. 保护会话密钥**    C. 保护明文    D. 以上都不对
76. 已知素数  $p$ , 以及  $\mathbb{Z}_p^*$  中的生成元  $g$ 。给定  $(p, g, g^x, g^y)$ , 求  $g^{xy}$ 。这被称作\_\_\_\_\_
- A. 大整数分解问题    B. 离散对数问题    C. 背包问题    **D. Diffie-Hellman 问题**
77. 下面属于 PKI 密钥生成周期的是\_\_\_\_\_
- A. 密钥保护    **B. 密钥使用**    C. 密钥泄露    D. 密钥封装
78. 关于安全协议说法不正确的是\_\_\_\_\_
- A. 必须事先估计各种不利条件  
 B. 不能假定一切都是正常的和非常理想的  
 C. 设计时, 有时考虑太全面反而无法实现  
**D. 无需考虑非法输入数据是否会导致异常的情况**
79. Dolev-Yao 攻击者模型中, 以下哪个是攻击者不能做到的\_\_\_\_\_
- A. 截获经过网络的任何消息    B. 有机会成为任何主体发出消息的接收者  
 C. 冒充任何别的主体给任意主体发消息    **D. 控制计算环境中的私有区域**
80. PGP 中使用的是哪个对称密码算法\_\_\_\_\_
- A. DES    **B. IDEA**    C. AES    D. KASUMI

## 二 判断

- |                                     |   |
|-------------------------------------|---|
| 1. 窃听属于主动攻击                         | × |
| 2. 柯克霍夫斯原则指出, 密码算法的安全性在于保密算法的细节     | × |
| 3. 真随机性是否存在属于哲学的范畴                  | ✓ |
| 4. 安全协议本身具有“高并发性”                   | ✓ |
| 5. 存在一个 15 阶的域                      | × |
| 6. AES 计算速度比 3DES 快, 且至少和 3DES 一样安全 | ✓ |
| 7. 篡改属于被动攻击                         | × |
| 8. 加密函数可以不是单射                       | × |
| 9. 量子力学告诉我们, 真随机性是存在的               | ✓ |
| 10. DES 的实际密钥长度只有 56 比特             | ✓ |

11. ElGamal 的安全性基于大整数分解问题	×
12. 存在一个 18 阶的域	×
13. AES 是作为 DES 的替代者被提出来的	√
14. 为安全起见, 在 RSA 加密前通常对明文进行随机填充	√
15. 一次一密中使用的密钥流在理论上是很容易破译的	×
16. 产生流密码中密钥流的一种主要工具是 FSR	√
17. Enigma 属于转轮机密码	√
18. 真随机具有不能可靠获得的性质	√
19. 数字信封中利用公钥密码保护数据, 对称密码保护解密密钥	×
20. 有限域又称伽罗瓦域	√
21. NP 问题是指无法解决的问题	×
22. 单向函数是否真的存在还是个未知数	√
23. 基于身份的密码学存在的问题有“私钥泄露了怎么办”	√
24. 有限域中的元素数量是有限的	√
25. 经过置换运算, 明文出现的字符一定出现在密文中	√
26. 电子计算机本身无法产生真正的随机数	√
27. 01011001101 比 10000001 更随机	×
28. 一次一密在商业中不太实用	√
29. $f(x)= x $ 不是单向函数	√
30. MAC 算法的安全性要求抗伪造	√
31. 相同阶的域都是同构的	×
PS: 正确答案: 相同阶的有限域都是同构的	
32. 公钥密码又称非对称密码	√
33. 不是所有的困难问题都能转化成密码体制	√
34. P 是否等于 NP 已经得到证明	×
35. 图灵机是用来描述算法这一概念的	√
36. 密钥空间要足够大, 以抵抗密钥的穷举攻击	√
37. 密钥可以根据个人喜好进行选取	×
38. 一次一密是绝对安全的	×
39. 排序问题是 P 问题, 所以也是 NP 问题	√
40. 提出 IBC 的原因是因为传统公钥密码不安全	×
41. 两军问题说明有些问题不存在完美的解决方案	√
42. PKI 是特指某一个密码设备和管理设施	×
43. 通过密文计算密钥, 至少要和计算明文一样困难	√
44. 即使设计上安全的密码算法, 在使用时也可能会不安全	√
45. 采用生日攻击时, 不需要考虑 Hash 函数的内部构造	√
46. 量子密码进入实用阶段后, 传统密码可以退休了	×
47. 存在一种方法, 可以将任一 NP 问题转换为密码体制	×
48. 对于(3,n)的门限方案, 恢复秘密信息最多需要三个人	×
49. S 盒是 DES 中唯一的线性部分	×
50. 数字信封是对称密码和公钥密码优点相结合的产物	√
51. 一个问题是 P 问题, 那它一定也是 NPC 问题	×
52. 单向函数可以用来构造加密体制	×
53. 量子密码的提出不是为了取代现有的密码体制	√

- |                              |   |
|------------------------------|---|
| 54. 双线性映射的主要优点是速度快           | × |
| 55. 实验“薛定谔的猫”是为了反驳哥本哈根解释而提出的 | √ |
| 56. ECC 的缺点是密钥相对较长           | × |
| 57. 基于超奇异椭圆曲线可以构造密码体制        | √ |
| 58. 公钥密码比对称密码更安全             | × |
| 59. “P 是 NP 的子集”已得到证明        | √ |
| 60. 设计安全协议时应考虑协议的并发特性        | √ |
| 61. 其实计算机就是一种图灵机             | × |
| 62. 好的安全协议需满足安全目标和理论目标       | × |
| 63. 不同阶的有限域绝对不可能同构           | √ |
| 64. 量子计算使得大整数分解问题不再困难        | √ |