

# 密码学原理 模拟试题(A)

一、单项选择题(每小题 1 分, 共 20 分). 段落标记

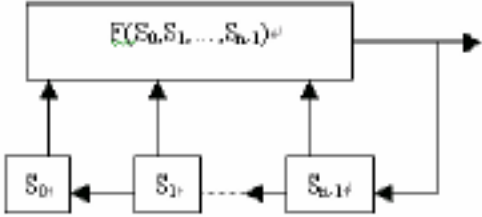
- 1976 年, 提出公开密码系统的美国学者是( )  
A、Bauer 和 Hill B、Diffie 和 Hellman C、Diffie 和 Bauer D、Hill 和 Hellman
- DES 算法中扩展运算 E 的功能是  
A、对 16 位的数据组的各位进行选择和排列, 产生一个 32 位的结果  
B、对 32 位的数据组的各位进行选择和排列, 产生一个 48 位的结果  
C、对 48 位的数据组的各位进行选择和排列, 产生一个 64 位的结果  
D、对 56 位的数据组的各位进行选择和排列, 产生一个 64 位的结果
- KASUMI 算法采用 Feistel 结构, 其安全性主要由轮函数提供, 轮函数包括  
A、非线性混合函数 FO 和非线性混合函数 FL 组成  
B、非线性混合函数 FO 和线性混合函数 FL 组成  
C、线性混合函数 FO 和线性混合函数 FL 组成  
D、线性混合函数 FO 和非线性混合函数 FL 组成
- 下表是 DES 算法中 S4 盒的选择矩阵, 如果其输入为 101011, 则输出为  

	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
0	7	13	14	3	0	6	9	10	1	2	8	5	11	12	4	15
1	13	8	11	5	6	15	0	3	4	7	2	12	1	10	14	9
2	10	6	9	0	12	11	7	13	15	1	3	14	5	2	8	4
3	3	15	0	6	10	1	13	8	9	4	5	11	12	7	2	14

  
A、0001 B、1010 C、1011 D、1100
- RSA 密码的安全性基于  
A、离散对数问题的困难性 B、子集和问题的困难性  
C、大的整数因子分解的困难性 D、线性编码的解码问题的困难性
- 如果某一个系统利用数字签名的方法来验证用户的口令, 则用户的口令是  
A、用户保密的解密密钥  $K_{di}$  B、用户公开的加密密钥  $K_{ei}$   
C、用户与系统共享的秘密密钥  $K$  D、以上说法都不对
- 报文的时间性认证是指  
A、接收者每收到一份报文后能够确认报文的发送时间  
B、接收者每收到一份报文后能够解密出报文的发送时间  
C、接收者每收到一份报文后能够确认报文是否保持正确的顺序、有无断漏和重复  
D、接收者每收到一份报文后能够确认报文是否按正确的时间发送

8、 如果一个置换密码使用下面的置换,则明文 abcdef 对应的密文为

1	2	3	4	5	6
3	5	1	6	4	2

- A、fedbca B、ceafdb C、edacfb D、cfdbae
- 9、 RIJNDAEL 算法中的许多运算是按字节定义的, 把一个字节看成是  
A、整数域上的一个元素 B、有限域  $GF(2^8)$  上的一个元素  
C、有限域  $GF(2)$  上的一个元素 D、有限域  $GF(2^{16})$  上的一个元素
- 10、目前公开密钥密码主要用来进行数字签名, 或用于保护传统密码的密钥, 而不主要用于数据加密, 主要因为  
A、公钥密码的密钥太短 B、公钥密码的效率比较低  
C、公钥密码的安全性不好 D、公钥密码抗攻击性比较差
- 11、一个密码系统如果用 E 表示加密运算, D 表示解密运算, M 表示明文, C 表示密文, 则下面哪个式子肯定成立  
A、 $E(E(M))=C$  B、 $D(E(M))=M$  C、 $D(E(M))=C$  D、 $D(D(M))=M$
- 12、如果 DES 加密使用的轮密钥为  $k_1, k_2, \dots, k_{16}$ , 则 DES 解密时第一轮使用的密钥为  
A、 $k_1$  B、 $k_8$  C、 $k_{12}$  D、 $k_{16}$
- 13、下图为移位寄存器的结构图
- 
- 如果  $F(s_0, s_1, \dots, s_{n-1})$  为线性函数, 则输出序列  
A、肯定为 m 序列 B、肯定为 M 序列 C、肯定为线性序列 D、肯定为非线性序列
- 14、在 ElGamal 密码中, 如果选择  $p = 11$ , 生成元  $\alpha = 2$ , 私钥为  $x = 8$ , 则其公钥为  
A、3 B、4 C、5 D、7

15、在 RSA 密码体制中，已知  $p = 3, q = 7$ , 同时选择  $e = 5$  则其私钥  $d$  为

- A、3                      B、4                      C、5                      D、6

16、假设某一个仿射密码中， $P = C = Z_{26}$ ， $n = 26$ ，如果其加密变换为  $e_k(x) = 7x + 3$ ，则其解密变换为

- A、 $d_k(y) = 15y - 19$                       B、 $d_k(y) = 7y + 3$   
C、 $d_k(y) = 7y - 3$                       D、 $d_k(y) = 15y + 19$

17、下面关于签名的说法中，那些是错误的

- A、为了安全，不要直接对数据进行签名，而应对数据的 HASH 值签名  
B、为了安全，要正确的选择签名算法的参数  
C、为了安全，应采用先签名后加密的方案  
D、为了安全，应采用先加密后签名的方案

18、下面的那种攻击不属于主动攻击

- A、窃听                      B、中断                      C、篡改                      D、伪造

19、把明文中的字母重新排列，字母本身不变，但位置改变了这样编成的密码称为

- A、代替密码                      B、置换密码                      C、代数密码                      D、仿射密码

20、KMC 或 KDC 主要负责

- A、密钥的产生                      B、密钥的分配                      C、密钥的销毁                      D、密钥的产生和分配

二、多项选择题 错选、多选不得分 每小题 2 分，共 10 分

1、香农建议密码设计的基本方法包括

- A、对合运算                      B、扩散                      C、混淆                      D、迭代

2、下列关于 IDEA 算法的描述中，正确的是

- A、IDEA 算法的加密过程由连续的 8 轮迭代和一个输出变换组成  
B、IDEA 算法的每一轮迭代中以 4 个 16 比特的子段作为输入，输出也是 4 个 16 比特的子段  
C、IDEA 算法的 9 轮迭代中，每一轮都需要 6 个 16 比特的子密钥  
D、IDEA 算法的明文、密文和密钥的长度都为 64 比特

3、盲签名与普通签名相比，其显著特点为

- A、签名者是用自己的公钥进行签名  
B、签名者不知道所签署的数据内容  
C、签名者先签名，然后再加密自己的签名，从而达到隐藏签名的目的  
D、在签名被接收者泄露后，签名者不能跟踪签名

4、一个好的口令应该满足

- A、应使用多种字符                      B、应有足够的长度                      C、应尽量随机                      D、应定期更换

5、由于传统的密码体制只有一个密钥，加密钥等于解密密钥，所以密钥分配过程中必须保证

- A、秘密性                      B、可用性                      C、真实性                      D、完整性

三、判断题 每小题 1 分，共 10 分

- 1、已知明文攻击是指密码分析者根据已知的某些明文-密文对来破译密码  
2、DES 算法中 S 盒是该算法中唯一的一种非线性运算  
3、3 个密钥的 3DES，总的密钥长度达到 168 位  
4、RIJNDAEL 算法不存在弱密钥和半若密钥，能有效抵抗目前已知的攻击  
5、传统密码既可提供保密性又可提供认证  
6、“一次一密”密码在理论上是绝对不可破译的  
7、凡是能够确保数据的真实性的公开密钥密码都可以用来实现数字签名  
8、目前影响电子政务、电子商务、电子金融应用的主要技术障碍是网络安全和信息安全问题

9、扩散指的是将每一位明文和密钥数字的影响扩散到尽可能多的密文数字中

10、盲签名比普通的数字签名的安全性要高

四、解释概念题 每小题 3 分，共 9 分

- 1、DES 弱密钥                      2、密钥托管加密                      3、NPC 问题

五、简答题 每小题 5 分，共 20 分

- 1、简述密码系统的组成                      2、简述认证和加密的区别                      3、简述公开密钥密码的基本思想

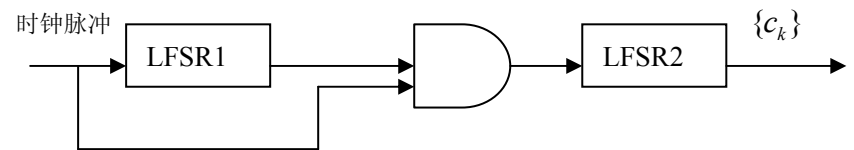
4、以  $c = m^e \bmod n$  为例，简述用“反复平方乘”计算大数的乘方运算的过程


六、计算题 每小题 10 分，共 20 分

1、在 DSS 数字签名标准中，取  $p = 11 = 2 \times 5 + 1$ ， $q = 5$ ， $h = 2$ ，于是  $g = 2^2 = 4 \bmod 11$ ，若取  $x = 3$ ，则  $y = g^x = 4^3 = 9 \bmod 11$  试对消息  $m = 7$  选择  $k = 3$  计算签名并进行验证

2、用 Fermat 费尔马 定理求  $3^{201} \bmod 11$

七、分析题 11 题 下图是一个简单的钟控序列的生成器，其中 LFSR1 和 LFSR2 分别为两个线性序列



在上图中  为与门，如果 LFSR1 为 2 级 m 序列  $\{a_k\} = 101101\dots$ ，LFSR2 为 3 级 m 序列

$\{b_k\} = 10011011001101\dots$ ，试确定该钟控序列生成器的输出序列  $\{c_k\}$  只写出前 10 位即可

## 密码学原理 模拟试题(A)参考答案

一、单项选择题(每小题1分, 共20分)

BBBAC ACBBB BDCAC ADABD

二、多项选择题 错选、多选不得分 每小题 2 分, 共 10 分

1、BCD 2、AB 3、BD 4、ABCD 5、ACD

三、判断题 每小题1分, 共10分

√√√√/ √√√√×

四、解释概念题 每小题 3 分, 共 9 分

复习资料 22.2; 25; 11

五、简答题 每小题 5 分, 共 20 分

复习资料 4; 75; 55; 60

六、计算题 每小题 10 分, 共 20 分

1、解、因为  $k=3$ , 所以有  $3^{-1} \bmod 5 = 2$

在进行数字签名时计算

$$r = ((g^k) \bmod p) \bmod q = (4^3 \bmod 11) \bmod 5 = 4$$

$$s = [(m + xr)k^{-1}] \bmod q = (7 + 3 \times 4)2 \bmod 5 = 3$$

所以消息  $m=7$  的签名为  $r, s = (4, 3)$

验证的过程如下

设用户收到的数据及签名为  $(m', r', s') = (7, 4, 3)$

首先计算  $w = (s')^{-1} \bmod q = 3^{-1} \bmod 5 = 2$

$$u_1 = [m'w] \bmod q = 7 \times 2 \bmod 5 = 4$$

$$u_2 = [r'w] \bmod q = 4 \times 2 \bmod 5 = 3$$

$$\begin{aligned} \gamma &= ((g^{u_1} y^{u_2}) \bmod p) \bmod q = ((4^4 9^3) \bmod 11) \bmod 5 \\ &= ((256 \times 729) \bmod 11) \bmod 5 = 9 \bmod 5 = 4 \end{aligned}$$

所以有  $\gamma = r'$  签名正确

2、解 根据 Fermat 定理有  $3^{10} \equiv 1 \bmod 11$ , 故

$$\begin{aligned} 3^{201} \bmod 11 &= 3^{200+1} \bmod 11 = (3^{200} \times 3) \bmod 11 \\ &= [(3^{200} \bmod 11) \times (3 \bmod 11)] \bmod 11 = [((3^{10})^{20} \bmod 11) \times 3] \bmod 11 \\ &= [((3^{10})^{20} \bmod 11) \times 3] \bmod 11 = [(3^{10} \bmod 11)^{20} \times 3] \bmod 11 \\ &= [1^{20} \times 3] \bmod 11 = 3. \end{aligned}$$

七、分析题 11 题

解 当LFSR1输出为1时, 移位时钟脉冲通过与门使LFSR2进行一次移位, 生成下一位, 如果LFSR1输出为0时, 移位时钟脉冲无法通过与门影响LFSR2, 所以LFSR2重复输出前一位, 所以其输出序列为 11000111011