密码学原理 模拟试题(C)

一、单项选择题(每小题 1 分，共 20 分).

1、 两个密钥的三重 DES，若其加密的过程为 $C = E_{k1}[D_{k2}[E_{k1}[P]]]$，其中 P 为明文，则解密的过程为

A、 $P = E_{k1}[D_{k2}[E_{k1}[C]]]$　　B、 $P = D_{k2}[D_{k1}[D_{k2}[C]]]$

C、 $P = D_{k1}[E_{k2}[D_{k1}[C]]]$　　D、 $C = D_{k2}[E_{k1}[D_{k2}[C]]]$

2、 IDEA 算法中关键非线性部件是乘/加 MA 单元，它的主要功能是

A、混淆　　B、扩散　　C、迭代　　D、以上答案都不对

3、 第三代移动通信国际组织(3GPP)规定了两个新的算法 f8 和 f9 作为标准，其中 f9 主要用来(　　)

A、加密　　B、认证　　C、密钥分配　　D、身份识别

4、 认证主要用来

A、确保数据的保密性

B、确保报文发送者和接收者的真实性以及报文的完整性

C、阻止对手的被动攻击

D、上说法都不对

5、 MD5 报文摘要算法是由 MIT 的 Ron Rivest 提出，其输出长度为

A、64 位　　B、128 位　　C、160 位　　D、192 位

6、 MD5 算法报文填充的目的是

A、使报文长度与 448 模 512 同余　　B、使报文长度为 512 的整数倍

C、使报文长度为 1024 的整数倍　　D、使报文长度与 448 模 1024 同余

7、 Diffe-Hellman 密钥分配方案的数学基础是

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

8、 CLIPPER 密码芯片使用的密码算法 SKIPJACK 属于分组密码，明文和密文分组长度为 64 位，密钥长度为

A、56　　B、64　　C、80　　D、128

9、 n 级线性移位寄存器不同的状态最多为

A、2^n　　**B**、2^n+1　　**C**、2^n-1　　**D**、2^{n+1}

10、同步序列密码是指

A、密钥序列的产生与密钥有关　　B、密钥序列的产生与密钥无关

C、密钥序列的产生与明文有关　　D、密钥序列的产生与明文无关

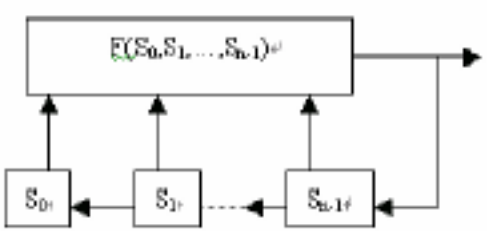
11、如果某系统利用单向函数实现一次性口令，假设用户 A 与用户 B 要进行通信，A 选择随机数 x 并计算 $y_0 = f^n(x)$，A 将 y_0 发给 B，用户 A 第 i 次通信的口令为

A、$y_i = f^i(x)$　　B、$y_i = f^{n-i}(x)$　　C、$y_i = f^n(x)$　　D、$y_i = f^{i+1}(x)$

12、在第三代移动通信系统中，以 KASUMI 算法为基础的 f_9 算法主要用来产生消息认证码，其中 KASUMI 算法的使用模式为

A、ECB 模式　　B、CBC 模式　　C、OFB 模式　　D、CFB 模式

13、下图为移位寄存器的结构图



如果 $F(s_0, s_1, ..., s_{n-1})$ 为非线性函数，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 BBS 随机数产生算法中，如果选取 $x_0 = x^2 \bmod n$ 作为该算法的种子　假定 n,x 已经满足要求 ，则随机数的第 i 位为

A、$x_i = {x_{i-1}}^2 \bmod n$ 的最高位　　B、$x_i = {x_{i-1}}^2 \bmod n + 1$ 的最高位

C、$x_i = {x_{i-1}}^2 \bmod n$ 的最低位　　D、$x_i = {x_{i-1}}^2 \bmod n + 1$ 的最低位

15、设散列函数 H 的输出为 m 比特，如果 H 的 k 个随机输入中至少有两个产生相同输出的概率大于 0.5,则 k 的值近似为

A、$2^{m/2}$　　B、$2^{m/4}$　　C、$2^{m/6}$　　D、$2^{m/8}$

16、AES 算法中的 S 盒是

A、8 位输入到 6 位输出的非线性变换　　B、8 位输入到 8 位输出的非线性变换

C、6 位输入到 6 位输出的非线性变换　　D、6 位输入到 8 位输出的非线性变换

17、CLIPPER 密码所使用的密钥中，那一个是在编程过程中产生的

A、FK 族密钥　　B、SN 芯片序列号　　C、UK 单元密钥　　D、Ks 会话密钥

18、下面关于 RSA 算法参数 p，q 的选择，那个是不恰当的

A、p，q 要足够大的素数　　B、p 和 q 的差的绝对值要小

C、p 和 q 要为强素数　　D、(p-1)和(q-1)的最大公因子要小

19、DES 算法经过了 16 轮迭代，每一轮需要一个轮密钥，轮密钥的长度为

A、32 位　　B、48 位　　C、56 位　　D、64 位

20、设散列函数 H 的输出为 m 比特，如果 H 的 k 个随机输入中至少有两个产生相同输出的概率大于 0.5,则 k 的值近似为

A、$2^{m/2}$　　B、$2^{m/4}$　　C、$2^{m/6}$　　D、$2^{m/8}$

二、多项选择题　错选、多选不得分　每小题 2 分，共 10 分

1、分组密码的短块加密方法主要有

A、填充法　　B、序列密码加密法　　C、输出反馈模式　　D、密文挪用技术

2、一种完善的签名应满足下面那些条件

A、签名者的签名应该被保密　　B、签名者事后不能抵赖自己的签名

C、签名不能被伪造　　D、签名可以通过仲裁机构来仲裁

3、下面那些方法可以用来产生报文认证码

A、序列号　　B、报文加密　　C、消息认证码　　D、散列函数

4、DES 算法的主要缺点有

A、密钥比较短　　B、存在弱密钥　　C、算法为对合运算　　D、存在互补对称性

5、KASUMI 算法设计的原则为

A、安全性要有足够的数学基础　　B、算法的软件实现要足够快，

C、算法的硬件实现要电路简单，功耗低　　D、算法必须采用 Feistel 网络结构

三、判断题　每小题 1 分，共 10 分

1、有限状态自动机密码是我国学者陶仁骥提出的

2、DES 算法中共有四个弱密钥

3、对于一个 n 级线性移位寄存器，至少有一种连接方式使其输出序列为 m 序列

4、根据密码分析者可以利用的资源来看，已知密文攻击是对密码分析者最不利的情况

5、如果一个密码，不能被密码分析者根据可利用的资源所破译，则称为是计算上不可破译的

6、RC4 密码是一种基于非线性数据表变换的序列密码

7、“一次一密”密码在实际应用中是行不通的，因为其密钥管理和密钥分配方面是非常困难的

8、如果采用相同长度的密钥，则椭圆曲线密码的安全性比 RSA 密码的安全性要高

9、如果用 AES 算法对 128 位的明文信息进行 10 轮加密，则圈密钥的总长为 1280 位

10、在公钥密码体制中，密钥的秘密性不需要保护

四、解释概念题　每小题 3 分，共 9 分

1、分组密码　　2、穷举攻击　　3、盲签名

五、简答题　每小题 5 分，共 20 分

1、 简述序列密码的基本思想

2、 试简述在 IDEA 算法的模乘运算中，为什么将模数取为 $2^{16}+1$ 而不是 2^{16}

3、 简述通过报文认证，通信双方能够确定那些内容？

4、 在不可否认签名算法中，为什么要包含一个否认协议？

六、计算题　每小题 10 分，共 20 分

1、在 ElGamal 密码体制中，设素数 p=71，本原根 g=7

1　如果接收方 B 的公开钥是 $y_B = 3$，发送方 A 选择的随机整数为 k=2,求明文 m=30 所对应的密文

2　如果用相同的 k=2 加密另外一个明文 m，加密后的密文为 C=（49，13），求 m

2、在 RSA 密码体制中，如果 p=3,q=7,n=pq=21,取公钥 e=5,如果明文消息为 m=8,试用该算法加密 m 得到密文 c，并解密进行验证

七、分析题　11 题　1、假定在置换密码中，其置换表如下

x	1	2	3	4	5	6	7	8
π(x)	4	1	6	2	7	3	8	5

1　求出逆置换表 $\pi^{-1}(x)$.

2　解密下面的密文

ETEGENLMDNTNEOORDAHATECOESAHLRMI

密码学原理 模拟试题(C)参考答案

一、单项选择题(每小题1分，共20分)

CBBBB AACAD BBDCA BCBBA

二、多项选择题 错选、多选不得分 每小题 2 分，共 10 分

1、ABD 2、BCD 3、BCD 4、ABD 5、ABC

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 6.1；7.1；71

五、简答题 每小题 5 分，共 20 分

复习资料 45；27(后面部分)；78(前面部分)；70

六、计算题 每小题 10 分，共 20 分

1、解 1 因为 k=2，所以 $u = y^k \bmod p = 3^2 \bmod 71 = 9$

$$c_1 = \alpha^k \bmod p = 7^2 \bmod 71 = 49$$

$$c_2 = um \bmod p = 9 \times 30 \bmod 71 = 57$$

所以 m=30 对应的密文为 49，57

2)，因为用同一个 k 加密不同的消息，所以有

$\frac{c_2}{c_2'} = \frac{m}{m'}$ 即 $\frac{57}{13} = \frac{30}{m'}$ 所以有 $57m' = 390 \bmod 71$

$$m' = 57^{-1} \times 390 \bmod 71 = 5 \times 390 \bmod 71 = 33$$

所以该明文消息为 m=33

2、解 因为 $p = 3, q = 7$ 所以有 $\Phi(n) = (p-1)(q-1) = 2 \times 6 = 12$

同时 $e^{-1} \bmod 12 = 5^{-1} \bmod 12 = 5$

所以明文消息 m=8 的密文为 $c = m^e \bmod n = 8^5 \bmod 21 = 8$

解密的过程如下 $m = c^d \bmod n = 8^5 \bmod 21 = 8$，

所以解密的结果为原来的明文

七、分析题 11 题

解 1 根据原置换表，其逆置换表如下

x	1	2	3	4	5	6	7	8
π^{-1}(x)	2	4	6	1	8	3	5	7

2 根据上面的逆置换表，可以得出该密文对应的明文为

Gentemendonotreadeachothersmail，

Gentle men do not read each other’s mail