*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

1、 1976 年，提出公开密码系统的美国学者是(B)

A、Bauer 和 Hill　B、Diffie 和 Hellman　C 、Diffie 和 Bauer　D、Hill 和 Hellman

2、 DES 算法中扩展运算 E 的功能是 B

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

3、 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 B

A、 非线性混合函数 FO 和非线性混合函数 F L 组成

B、 非线性混合函数 FO 和线性混合函数 F L 组成

C、 线性混合函数 FO 和线性混合函数 F L 组成

D、 线性混合函数 FO 和非线性混合函数 F L 组成

4、 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 A

	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

5、 RSA 密码的安全性基于 C

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

6、 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

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

7、 报文的时间性认证是指 C

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 B

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 B

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 B

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

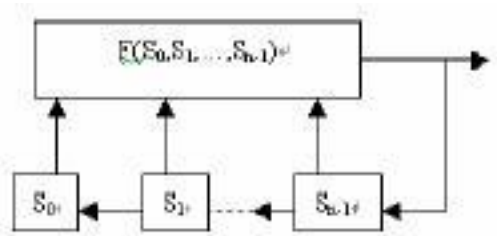
11、一个密码系统如果用 E 表示加密运算，D 表示解密运算，M 表示明文，C 表示密文，则下面哪个式子肯定成立 B

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 $k_1, k_2, ..., k_{16}$，则 DES 解密时第一轮使用的密钥为 D

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 C



如果 $F(s_0, s_1, ..., s_{n-1})$ 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 = 2，私钥为 x = 8，则其公钥为 A

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 C

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

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 D

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

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 B

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 D

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

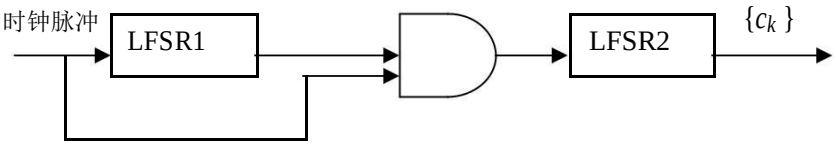
4、以 $c=m^e \bmod n$ 为例，简述用“反复平方乘”计算大数的乘方运算的过程

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=2×5+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 D 为与门，如果 LFSR1 为 2 级 m 序列 $\{a_k\}=101101.....$,LFSR2 为 3 级 m 序列 $\{b_k\}=10011011001101....$，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)

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

22222 2222×

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

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

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

$$= ((g^{u_1} y^{u_2}) \bmod p) \bmod q = ((4^{4}9^{3}) \bmod 11) \bmod 5$$

$$= ((256 \times 729) \bmod 11) \bmod 5 = 9 \bmod 5 = 4$$

所以有　$= r'$ 签名正确

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

$$3^{201} \bmod 11 = 3^{200+1} \bmod 11 = (3^{200} \times 3) \bmod 11$$

$$= [(3^{200} \bmod 11) \times (3 \bmod 11)] \bmod 11 = [((3^{10})^{20} \bmod 11) \times 3] \bmod 11 = [((3^{10})^{20} \bmod 11) \times 3] \bmod 11 = [(3^{10} \bmod 11)^{20} \times 3] \bmod 11$$

$$= [1^{20} \times 3] \bmod 11 = 3.$$

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\

密码学原理 模拟试题(B)

DABBD BCCAC BDBAD BABBC

一、单项选择题(每小题 1 分，共 20 分).

1、 l998 年 8 月 20 日，美国国家标准技术研究所(NIST)召开了第一次 AES 候选会议 同时公布的符合基本要求的候选算法有(D)

A 5 个 B 6 个 C、10 个 D、l5 个

2、 AES 算法中的状态可表为一个二维数组，如果明文长度为 128 比特，则明文状态为 A

A、4 行 4 列 **B、**4 行 6 列 C、4 行 8 列 D、4 行 10 列

3、 设一个公开密钥密码的加密运算为 E，解密运算为 D，加密密钥为 K_e，解密密钥为 K_d，t 为明文消息，如果要确保数据的真实性，则发送方要发送的密文为 B

A、 $E(M, K_e)$ B、 $D(M, k_d)$ C、 $E(M, K_d)$ D、 $D(M, k_e)$

4、 如果 hash 函数的函数值为 64 位，则对其进行生日攻击的代价为 B

A、 2^{16} B、 2^{32} C、 2^{48} D、 2^{64}

5、 如果用 DES 算法实现一次性口令，系统产生的随机数为 R，并加密 R 得到 E(R,K)，然后将 E(R,K) k 为用户与系统之间共享的秘密密钥 发送给用户，则用户的口令为 D

A、E(R,k)+1 B、E(D(E(R,k),k),k) C、D(E(R,K),K)+1 D、E(D(E(R,K),K)+1,K)

6、 著名的 Kerckhoff 原则是指 B

A、系统的保密性不但依赖于对加密体制或算法的保密，而且依赖于密钥

B、系统的保密性不依赖于对加密体制或算法的保密，而依赖于密钥

C、系统的保密性既不依赖于对加密体制或算法的保密，也不依赖于密钥

D、系统的保密性只与其使用的安全算法的复杂性有关

7、 下面那种密码可以抵抗频率分析攻击 C

A、置换密码 B、仿射密码 C、多名代替密码 D、加法密码

8、 一个数字签名体制都要包括 c

A、加密和解密两个方面 B、加密和认证两个方面

C、施加签名和验证签名两个方面 D、认证和身份识别两个方面

9、 《保密系统的通信理论》这篇论文把密码学置于坚实的数学基础之上，标志着密码学作为一门学科的形成，该论文的作者是 A

A、香农 B、图灵 C、布尔 D、W. Diffie

10、下面关于 AES 算法的叙述，那一个是正确的 (C)

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 位、192 位或 256 位的分组密码算法 D、AES 是一个数据块长度和密钥长度可分别为 64 位或 128 位的分组密码算法

11、如果一个置换密码系统使用下面的置换 B

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

则其逆置换为

A

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

B、

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

C、

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

D、

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

12、在一般的英文语言中，出现频率最高的字母为 D

A、O B、T C、 A D、E

13、如果签名者为 A，对 RSA 数字签名的一般攻击方法为 B

A、攻击者随意选择一个 Y，计算 $X = (Y)^e \bmod n$，则 X 是 A 对 Y 的一个有效的签名 B、攻击者随意选择一个 Y，计算 $X = (Y)^e \bmod n$，则 Y 是 A 对 X 的一个有效的签名 C、攻击者随意选择一个 Y，计算 $X = (Y)^d \bmod n$，则 X 是 A 对 Y 的一个有效的签名 d A

14、对于一个给定的散列函数 H，其单向性是指 D

A、对于给定的 hash 码 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 $y\ x$ 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)的偶对(x，y)在计算上是不可行的 D、以上说法都不对

15、安全 hash 算法(SHA)输出报文摘要的长度为 D

A、120 B、128 C、144 D、160

16、有一个三级非线性反馈移位寄存器，反馈函数为 $f(s_0, s_1, s_2) = s_0\ \ s_2\ \ 1\ \ s_1 s_2$，且初始状态为 000，则该移位寄存器产生的序列的前 4 位为 B

A、0010 B、1011 C、1111 D、1010

17、如果 M, C, K 分别表示明文，密文，和密钥，而 M', C', K' 分别表示 M, C, K 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

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 $C' = E(M', K)$

18、在不可否认签名中，如果签名者不执行否认协议，则表明 B

A、签名是假的 B、签名是真实的 C、无法判断真假 D、该签名无效

19、设某一移位密码体制中， $P = C = Z_{26}, 0 \quad k \quad 25,$ 定义 $e_k(x) = x + k \bmod 26,$ 同时 $d_k(y) = y \quad k \bmod 26, x, y \quad Z_{26}$，如果取 $k = 11$，则明文 will 的密文为 B

A、xepp B、htww C、midd D、torr

20、下面关于站点认证的说法中，错误的是 C

A、站点认证是要认证通信是否在意定的两个站点之间进行

B、站点认证是通过验证加密的数据能否成功的在两个站点之间进行传送来实现

C、站点认证只能用对称密钥密码进行

D、站点认证即可以用对称密钥密码进行，也可以用公开密钥密码进行

二、多项选择题 错选、多选不得分 每小题 2 分，共 10 分

1、RIJNDAEL 算法中的轮函数由下面的那些运算部件组成 abcd

A、行移位 B、字节代换 C、列混合 D、密钥加

2、链接技术是一种掩盖明文数据模式的有效方法，下面关于链接技术正确的说法是 abd

A、 链接是算法的当前输出不仅与当前的输入和密钥有关，而且还与以前的输入与输出有关

B、 采用链接技术，即使明文和密钥相同，所产生的密文也可能不相同

C、 采用链接技术，如果明文和密钥相同，所产生的密文也一定不相同

D、 会产生错误传播

3、公钥密码体制的基本思想包括 acd

A、 将传统密码的密钥一分为二，分为加密密钥 k_e 和解密密钥 k_d B、 k_e 由加密方确定， k_d 由解密方确定

C、 由加密密钥 k_e 推出解密密钥 k_d 在计算上是不可行的 D、 k_e 公开， k_d 保密

4、身份识别对确保系统的安全是极其重要的，下面那些方法可以用来进行用户身份认证 acd

A、 用户知道什么 B、用户能做什么 C、用户拥有什么 D、用户的生理特征

5、DES 算法的 S 盒满足下面的那些准则 abd

A、 输出不是输入的线性和仿射函数

B、 任意改变输入中的 1 位，输出中至少有 2 位发生变化

C、 任意改变输入中的 1 位，输出中至少有 3 位发生变化

D、 保持输入中的 1 位不变，其余 5 位变化，输出中的 0 和 1 的个数接近相等

三、判断题 每小题 1 分，共 10 分

1、DES 算法存在弱密钥，但不存在半弱密钥

2、为了序列密码的安全，应使用尽可能长的密钥

3、SKIPJACK 算法不是对合运算，所以加密和解密过程不一致

4、如果一个密码，无论密码分析者截获了多少密文和用什么技术方法进行攻击都不能被攻破，则称为是绝对不可破译的

5、对于 CLIPPER 密码算法，如果需要，可经法律部门许可破译密码进行监听

6、Vernam 密码不属于序列密码

7、DES 算法是面向二进制的密码算法，所以可以加解密任何形式的计算机数据

8、Hash 函数要能够用于报文认证，它必须可应用于任意大小的数据块并产生定长的输出

9、M 序列的 0，1 分布及游程分组都是均匀的，而且周期达到最大

10、RIJNDAEL 算法在整体结构上采用的是代替－置换网络构成圈函数，多圈迭代

四、解释概念题 每小题 3 分，共 9 分

1、单钥密码体制 2、扩散 3、PKC

五、简答题 每小题 5 分，共 20 分

1、简述密码技术的基本思想 2、试简述 DES 算法的加密过程

3、简述认证和数字签名的区别 4、在 DSA 签字算法中，参数 k 泄露会产生什么后果?

六、计算题 每小题 10 分，共 20 分

1、Diffie-Hellman 密钥交换过程中，设大素数 p=11， =2 是 Z_p 的本原元，用户 U 选择的随机数是 5 用户 V 选择的随机数是 7，试确定 U 和 V 之间共享的密钥

2、在 BBS 随机数产生算法中，选择 p=5,q=7,n=pq=35,如果取 x=11,试计算出由该算法生成的序列的前 5 位

七、分析题 11 题 在公钥体制中，每一用户 U 都有自己的公开钥 pk_u 和秘密钥 sk_u 如果任意两个用户 A、B 按以下方式通信，A 发给 B 消息 $(E_{pkB}(m), ID_A)$，B 收到后，自动向 A 返回消息 $(E_{pkA}(m), ID_B)$，以使 A 知道 B 确实收到报文 m 问用户 C 怎样通过攻击手段获取报文 m? 假设两个用户有相同的 n

*密码学原理*模拟试题(B)参考答案

一、单项选择题(每小题 1 分，共 20 分)

DABBD　BCCAC　BDBAD　BABBC

二、多项选择题　错选、多选不得分　每小题 2 分，共 10 分

1、ABCD　　2、ABD　　3、ACD　　4、ACD　　5、ABD

三、判断题　每小题 1 分，共 10 分

×5555　　×5555

四、解释概念题　每小题 3 分，共 9 分

复习资料　5　前面部分）；10 1；89

五、简答题　每小题 5 分，共 20 分

复习资料　2；18；75；68

六、计算题　每小题 10 分，共 20 分

1、解　用户 U 计算出 $2^5 \bmod 11 = 10$ 发送给 V，用户 V 计算出 $2^7 \bmod 11 = 7$ 发送

U，

= U 可以计算出密钥 $7^5 \bmod 11 = 10$，

= 可以计算出密钥 $10^7 \bmod 11 = 10 \bmod 11 = 10$，

所以双方共享的密钥为 10

2、根据 BBS 随机数产生的算法有

$$x_0 = x^2 \bmod n = 11^2 \bmod 35 = 16$$

所以有　$x_1 = x_0{}^2 \bmod n = 16^2 \bmod 35 = 11$　该序列的第一位为 x_1 的最低位 1

$x_2 = x_1{}^2 \bmod n = 11^2 \bmod 35 = 16$　该序列的第二位为 x_2 的最低位 0

$x_3 = x_2{}^2 \bmod n = 16^2 \bmod 35 = 11$　该序列的第三位为 x_3 的最低位 1

$x_4 = x_3{}^2 \bmod n = 11^2 \bmod 35 = 16$　该序列的第四位为 x_4 的最低位 0

$x_5 = x_4{}^2 \bmod n = 16^2 \bmod 35 = 11$　该序列的第五位为 x_5 的最低位 1

所以该 BBS 算法产生的前五位为 10101

七、分析题　11 题

解　用户 C 攻击的过程如下　令 $c_1 = E_{pk_A}(m) c_2 = E_{pk_B}(m)$

攻击者 C 可以在信道中截获 c_1 和 c_2　同时由于 pk_A 和 pk_B 是公开的，所以 C 可以

知道　且 pk_A 和 pk_B 是互素的　一般情况都满足），则 C 使用推广的欧几里得算

法可以求出满足 $rpk_A + spk_B = 1$ 的 r 和 s，这两个数一个为负，另一个为正　假

设 r 为负，则用户 C 可以求出 $c_1{}^1 \bmod n$，然后用下面的式子计算出 m

$(c_1{}^{-1})$　$r \quad c_2{}^s = m^{rpk_A + spk_B} \bmod n = m \bmod n = m$

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

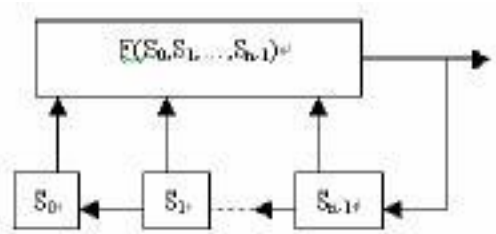
11、如果某系统利用单向函数实现一次性口令，假设用户 A 与用户 B 要进行通信，A 选择随机数 x 并计算 $y_0 = f^n(x)$，A 将 y_0 发给 B，用户 A 第 i 次通信的口令为

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

33333 333××

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 $u = y^k \bmod p = 3^2 \bmod 71 = 9$

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

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

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 $\frac{7}{13} = \frac{30}{m}$ 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 $(n) = (p-1)(q-1) = 2 \times 6 = 12$

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
$\pi^{-1}(x)$	2	4	6	1	8	3	5	7

u 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

《应用密码学》试题

一、简单题（40 分）

1. 简述密码学发展的三个阶段及其主要特点。

答题要点：密码学的发展大致经历了三个阶段：

（1）古代加密方法。特点：作为密码学发展的起始阶段，所用方法简单，体现了后来发展起来的密码学的若干要素，但只能限制在一定范围内使用。主要基于手工的方式实现。

（2）古典密码。特点：加密方法一般是文字置换，使用手工或机械变换的方式实现。古典密码系统已经初步体现出近代密码系统的雏形，它比古代加密方法更复杂，但其变化量仍然 比较小。转轮机的出现是这一阶段的重要标志，传统密码学有了很大的进展，利用机械转轮可以开发出极其复杂的加密系统，缺点是密码周期有限、制造费用高等。

（3）近代密码。特点：这一阶段密码技术开始形成一门科学，利用电子计算机可以设计出 更为复杂的密码系统，密码理论蓬勃发展，密码算法设计与分析互相促进，出现了大量的密 码算法和各种攻击方法。另外，密码使用的范围也在不断扩张，而且出现了以 DES 为代表的 对称密码体制和 RSA 为代表的非对称密码体制，制定了许多通用的加密标准，促进网络和 技术的发展。

2. 密码学的五元组是什么？它们分别有什么含义？

答：密码学的五元组是指：｛明文、密文、密钥、加密算法、解密算法｝。

明文：是作为加密输入的原始信息，即消息的原始形式，通常用 m 或表示。

密文：是明文经加密变换后的结果，即消息被加密处理后的形式，通常用 c 表示。

密钥：是参与密码变换的参数，通常用 k 表示。

加密算法：是将明文变换为密文的变换函数，相应的变换过程称为加密，即编码的过程，通常用表示，即 $c\ E_k\ p$ 。

解密算法：是将密文恢复为明文的变换函数，相应的变换过程称为解密，即解码的过程，通常用 D 表示，即 $p\ D_k\ c$ 。

3. 从运行条件和安全条件两个方面比较常规密码体制和公开密钥密码体制并列举典型的

分类	常规密码体制	公开密钥密码体制
运行条件	加密和解密使用同一个密钥和同一个算法。	用同一个算法进行加密和解密，而密钥有一对，其中一个用于加密，另一个用于解密。
	发送方和接收方必须共享密钥和算法。	发送方和接收方每个使用一对相互匹配、而又彼此互异的密钥中的一个。
安全条件	密钥必须保密。	密钥对中的私钥必须保密。
	如果不掌握其他信息，要想解密报文是不可能或至少是不现实的。	如果不掌握其他信息，要想解密报文是不可能或者至少是不现实的。
	知道所用的算法加上密文的样本必须不足以确定密钥。	知道所用的算法、公钥和密文的样本必须不足以确定私钥。

4. 解释群、交换群、有限群、有限群的阶、循环群、生成元、域、有限域、不可约多项式并举例说明。

答：群由一个非空集合 G 组成，在集合 G 中定义了一个二元运算符“· ”，满足：

= 封闭性：对任意的 $a, b \ G$，有：$a \ b \ G$；

= 结合律：对任何的 $a, b, c \ G$，有：$a \ b \ c \ a \ b \ c \ a \ b \ c$；

= 单位元：存在一个元素 $1 \ G$ (称为单位元)，对任意元素，有：$a \ 1 \ 1 \ a \ a$；

= 逆元：对任意 $a \ G$，存在一个元素 $a^{1} \ G$ (称为逆元)，使得：$a \ a^{1} \ a^{1} \ a \ 1$。

如果一个群满足交换律，则称其为交换群。

如果一个群的元素是有限的，则称该群为有限群。

有限群的阶就是群中元素的个数。

如果群中每一个元素都是某一个元素 $a \ G$ 的幂 $a^{k} \ G$ (k 为整数)，则称该群是循环群。

在循环群中，认为元素 a 生成了群 G，或 a 是群 G 的生成元。

域是由一个非空集合 F 组成，在集合 F 中定义了两个二元运算符：“+”(加法)和“· ”(乘法)，并满足：

(1) F 关于加法“+”是一个交换群；其单位元为“0”，a 的逆元为 a。

(2) F 关于乘法“· ”是一个交换群；其单位元为“1”，a 的逆元为 a^{1}。

(3)(分配律)对任何的 $a, b, c \ F$，有：$a \ (b \ c) \ b \ c \ a \ a \ b \ a \ c$；

(4)(无零因子)对任意的 $a, b \ F$，如果 $a \ b \ 0$，则 $a \ 0$ 或 $b \ 0$。

如果域 F 只包含有限个元素，则称其为有限域。

不可约多项式是指不能再分解为两个次数低于该多项式最高次的多项之积的多项式。

5. 画出分组密码算法的原理框图，并解释其基本工作原理。

答：

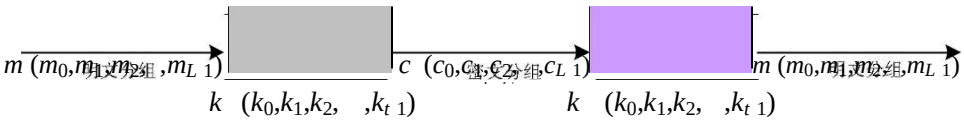


图5-1 分组密码原理框图

分组密码处理的单位是一组明文，即将明文消息编码后的数字序列 $m_0, m_1, m_2, , m_i$ 划分成长为 L 位的组 $m \ m_0, m_1, m_2, , m_{L \ 1}$，各个长为 L 的分组分别在密钥 $k \ k_0, k_1, k_2, , k_{t \ 1}$（密钥长为 t）的控制下变换成与明文组等长的一组密文输出数字序列 $c \ c_0, c_1, c_2, , c_{L \ 1}$。$L$ 通常为 64 或 128。解密过程是加密的逆过程。

$$x \equiv 2 \pmod 3$$

二、（15 分）求解： $x \equiv 1 \pmod 5$

$$x \equiv 1 \pmod 7$$

解： M = 3×5×7 = 105; M/3 = 35; M/5 = 21; M/7 = 15。

35b1＝1 (mod 3)

21b2＝ 1 (mod 5)

15b3＝1 (mod 7)

因此有： b1 = 2; b2 = 1; b3 = 1。

则：x ＝2×2×35 + 1×1×21 + 1×1×15＝176 (mod 105)＝71

三、（15 分）用 Hill 密码加密明文“pay more money”,密钥是： $k = \begin{matrix} 17 & 17 & 5 \\ 21 & 18 & 21 \\ 2 & 2 & 19 \end{matrix}$

解：明文“pay more money”可编码为：15 0　24；12 14 17；4　12　14；13 4 24。

由于：

$$\begin{matrix} 17 & 17 & 5 \\ 21 & 18 & 21 \\ 2 & 2 & 19 \end{matrix} \begin{matrix} 15 \\ 0 \\ 24 \end{matrix} = \begin{matrix} 303 \\ 303 \\ 531 \end{matrix} \bmod 26 = [17\ 17\ 11]$$

$$\begin{matrix} 17 & 17 & 5 \\ 21 & 18 & 21 \\ 2 & 2 & 19 \end{matrix} \begin{matrix} 12 \\ 14 \\ 17 \end{matrix} = \begin{matrix} 532 \\ 490 \\ 677 \end{matrix} \bmod 26 = [12\ 22\ 1]$$

$$\begin{matrix} 17 & 17 & 5 \\ 21 & 18 & 21 \\ 2 & 2 & 19 \end{matrix} \begin{matrix} 4 \\ 12 \\ 14 \end{matrix} = \begin{matrix} 348 \\ 312 \\ 538 \end{matrix} \bmod 26 = [10\ 0\ 18]$$

$$\begin{matrix} 17 & 17 & 5 \\ 21 & 18 & 21 \\ 2 & 2 & 19 \end{matrix} \begin{matrix} 13 \\ 4 \\ 24 \end{matrix} = \begin{matrix} 353 \\ 341 \\ 605 \end{matrix} \bmod 26 = [15\ 3\ 7]$$

故对应的密文为：RRLMWBKASPDH。

四、（15 分）设通信双方使用 RSA 加密体制，接收方的公开密钥是（5,35），接收到的密文是 10，求明文。

解：据题意知：e ＝5，n ＝35，C ＝10。

因此有：　n　35　5　7　4　6　24

$d\ e^{-1} \bmod n \ \ 5^{-1} \bmod 24 \ \ 5$

所以有：$M \ \ C^{d} \bmod n \ \ 10^{5} \bmod 35 \ \ 5$ 。

五（、15 分）利用椭圆曲线实现 ElGamal 密码体制，设椭圆曲线是 $E_{11}(1,6)$，生成元 $G(2,7)$，接收方 A 的秘密密钥 n_A 7 。求：

（1）A 的公开密钥 P_A 。

（2）发送方 B 欲发送消息 P_m (10,9)，选择随机数 k 3，求密文 C_m 。

（3）显示接收方 A 从密文 C_m 恢复消息 P_m 的计算过程。

解：（1） $P_A = n_A \times G = 7 \times (2,7) = (7,2)$ 。

（2）
$$C_m = \{kG, P_m + kP_A\} = \{3(2,7), (10,9) + 3(7,2)\}$$
$$= \{(8,3), (10,9) + (3,5)\}$$
$$= \{(8,3), (10,2)\}$$

（3） $P_m = (10,2) - 7(8,3) = (10,2) - (3,5) = (10,2) + (3,6) = (10,9)$ 。