部分习题集答案

第四题　综合问答题

1、维吉尼亚密码体制的考查

（1）解密函数 D_k 和加密函数 E_k 一样，假设密文 $c=(c_1, c_2, \ldots, c_n)$，则解密函数为：

$D_k(c_1, c_2, \ldots, c_n)=((c_1-k_1) \bmod 26，(c_2-k_2) \bmod 26，\ldots，(c_n-k_n) \bmod 26$

$= m_1, m_2, \ldots, m_n$

（2）明文字符 b 对应 1，y 对应 24，e 对应 4

加密过程为：$c_1=1+5 \bmod 26 =6$　$c_2=24+2 \bmod 26=0$　$c_3=4+1 \bmod 26=5$。

2、此题是对 DES 算法的考核，共 2 题。（共 6 分）

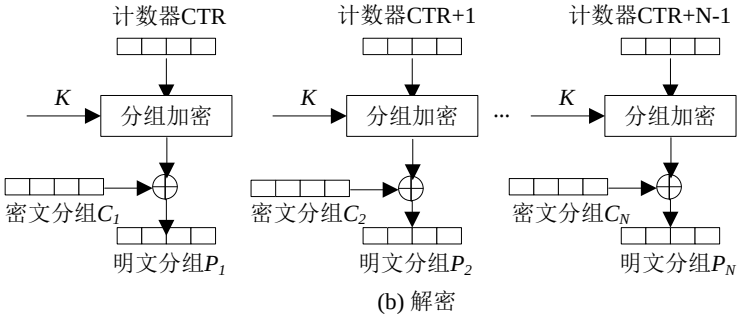
（1）完成题目中的填空；

①　E 盒扩展　；　②　S 盒压缩　；③　P 盒替代　。

（2）下图 3 是 S 盒中的 S_1，如果输入为（111011），则输出应为___0 ___

3、此题是对分组密码的工作模式考查，共 2 题。

（1）CTR 解密运行过程如下：



(b) 解密

CTR 运行模式解密过程示意图

（2）会影响 3 组的密文分组无法正常解密

4、此题是对 RSA 算法考查，共 2 题。

（1）完成题目中的填空；

①_____{e=7，n=143}____；　②_____{d=103，n=143}_____；

（2）假设发送的消息 m=4，求 Alice 接收得密文 c。（给出详细求解过程）

解：密文： $c=m^e \bmod n$ （1 分） $c=4^7 \bmod 143$

$c=(2^8)*(2^6) \bmod 143$

$c=82$

5、下题是对 SHA-1 算法考查，包含了 2 个小题。

（1)给出第二部分填充消息的比特位长度？第三部分数据长度的比特位长度？

解：填充公式： $l+1+k \equiv 448 (\bmod 512)$

l=8*8=64， 448-64=384，因此第二部分填充消息的比特位长度为 384 。

第三部分数据长度的比特位长度为 64

（2）消息填充之后，输出第 0 组 W[0]，第 1 组 W[1]，第 2 组 W[2]。（十六进制表示）

解：其中 a 的十六进制为 61，b 为 62 c 为 63 d 为 64 0 为 30 1 为 31 2 为 32 3 为 33

因此 W[0]=61626364 w[1]= 30313233 w[2]=80000000

6. 仿射密码算法

解密公式为：$x= k^{-1}(y-b) \bmod 26$

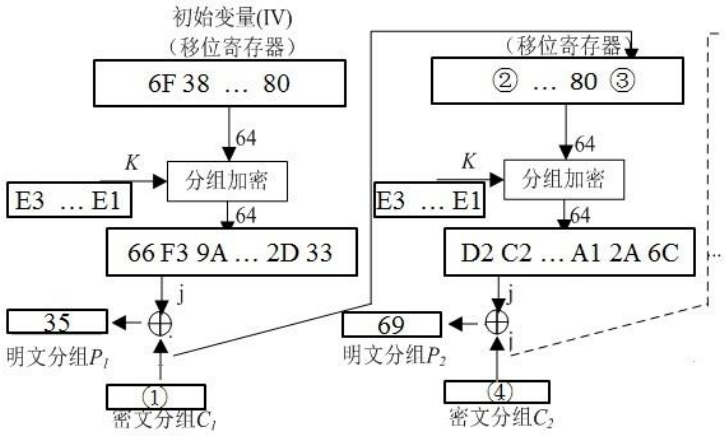
明文字符 c 对应 2，加密过程为：$y=17\times 2+11 \bmod 26=19$。

7. 按箭头顺序依次为：轮密钥加、字节替代、行移位、列混合、轮密钥加、字节替代、行移位、轮密钥加。

字节替代、行移位各执行 10 次，轮密钥加 11 次，列混合 9 次。

8. CFB

①35H⊕66H=53H ②38H ③53H ④BBH



9. E 扩展，E 盒的输入为 16 进制的{EA09782C}

0	1	1	1	0	**1**
0	1	0	1	0	**0**
0	0	0	0	0	**1**
0	1	0	0	1	**0**
1	0	1	1	1	**1**
1	1	0	0	0	**0**
0	0	0	1	0	**1**
0	1	1	0	0	1

10. Diffie-Hellman 密钥交换算法 参考答案：

$K=6^{11\times27} \bmod 41=6^{297} \bmod 41$

由欧拉定理，$6^{40} \bmod 41\equiv1$

故 $6^{297} \bmod 41\equiv6^{17} \bmod 41$

$6^2 \bmod 41\equiv36\equiv-5$　$6^4 \bmod 41\equiv25$　$6^8 \bmod 41\equiv10$　$6^{16} \bmod 41\equiv18$

故 $6^{17} \bmod 41\equiv18\times6\equiv26$

11、DES 的考核

解：（1）S 盒压缩和 P 盒置换的输出是 32bits，E 盒扩展和 E 盒与轮密钥异或的输出是 48bits

（2）6（或者 0110））

12、 AES 算法考核

解： （1）

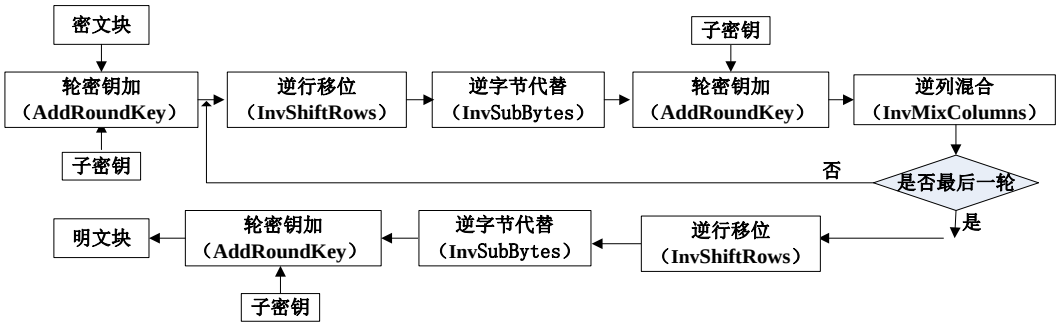


图 1　AES 解密过程

（2）128bits 需要扩展密钥长度是 11*128-128=1280bits

192bits 需要扩展密钥长度是 13*128-192=1472bits

256bits 需要扩展密钥长度是 15*128-256=1664bits

13、OFB 工作模式考核（共 8 分）

解：（1）

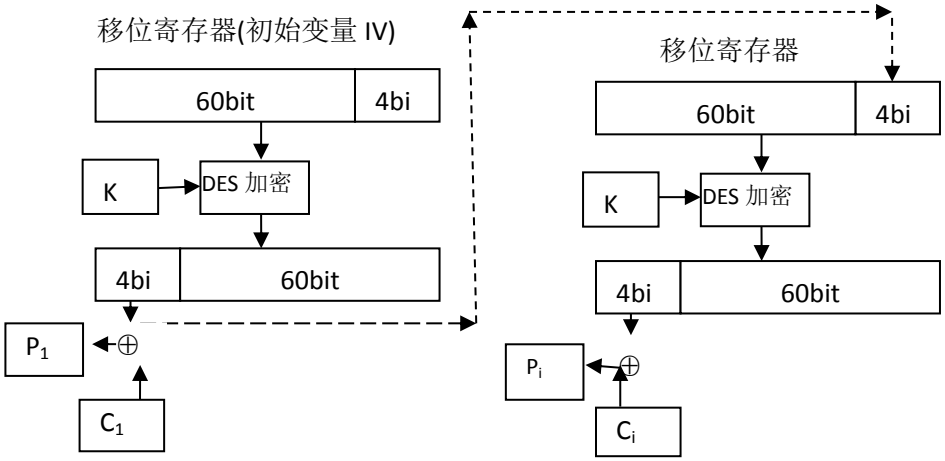


图 2 OFB 工作模式解密图

（2）OFB 工作模式下，DES 密钥流生成器是属于同步流密码，密（明）文符号是独立的，明文和密文一个错误传输只会影响一个符号，不影响后面的符号。

14、序列密码考核（共 6 分）

解： （1） 4 级线性移位寄存器的反馈函数为 $f(a_1,a_2,a_3,a_4)=a_1\oplus a_2\oplus a_4$，

因此对应特征多项式为 $f(x)=x^4+x^3+x+1$

特征多项式不是本原多项式，不是 m 序列

因为 $x^6-1=(x^2-x-1)(x^4+x^3+x+1)$，即 $x^4+x^3+x+1\,|\,x^6-1$

最小整数为 6，即周期为 6

（2）画出 LFSR 反馈状态图

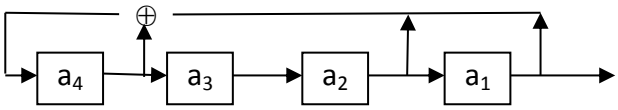


图 3 4 级线性反馈移位寄存器状态图

15、消息认证知识点考核 （共 6 分）

解：（1） 解密算法 D、Message、Message、Mac 算法（C）

（2）这消息认证模式能达到信息安全目标中完整性、保密性

16、DES 的考核

解：“itis2015”转换为 ASCII 值分别为

i 105 01101001 t 116 01110100 i 105 01101001 s 115 01110011

2 50 00110010 0 48 00110000 1 49 00110001 5 53 00110101

经过 IP 初始置换之后的值

01101001
01110100
01101001
01110011
00110010
00110000
00110001
00110101

58	50	42	34	26	18	10	2
60	52	44	36	28	20	12	4
62	54	46	38	30	22	14	6
64	56	48	40	32	24	16	8
57	49	41	33	25	17	9	1
59	51	43	35	27	19	11	3
61	53	45	37	29	21	13	5
63	55	47	39	31	23	15	7

IP 置换的输出的后 4 行分别为输入的 第 1 列，第 3 列，第 5 列， 第 7 列，每列次序颠倒，因此后 4 行分别为：

0	0	0	0	0	0	0	0
1	1	1	1	1	1	1	1
0	0	0	0	0	1	0	1
0	0	0	1	1	0	0	0

十六进制为：0x00FF0518

17、SHA-1 函数考核 （共 6 分）

解：（1）一个分组 512 比特，则 512/8=64 字节，199/64≈3，因此总共分组 4 个分组

最后一分组的消息长度 199 mod 64= 7，另外有 64bits，即 8 字节作为数据长度，因此填充消息长度为 64-7-8=49 字节

（2）若消息的长度为 252 字节，按照 SHA-1 算法的规定，需要对消息进行分组和填充. 252/64≈3, 252 mod 64=60，因此总共 5 个 512bits 块，一个 512bits 分组总共 80 个轮次，5 个 512bits 则需要运行 400 次 SHA-1 压缩函数

18、 AES 算法考核

解： （1）有限域加法运算为异或运算

因此 *F0+E9=0x19*

（2）*16* 进制的*“03”*与*“80”*的乘法，即计算*“03•80”*的值。

“03” 等价于多项式是“x+1”，*“80”*等价于“x^7”

（x+1）$x^7=x^8+x^7$（mod $x^8+x^4+x^3+x+1$）

≡（$x^8+x^4+x^3+x+1$）+ $x^7+x^4+x^3+x+1$

≡$x^7+x^4+x^3+x+1$

“03•80”=10011011=0x9b

备注：此题也采用其它计算方法

19、OFB 工作模式考核

解：（1）AES 明文长度 128bits,即 16 字节，因此分组长度为：

2200/16=137.5

即 2200 分组有 138 个明文分组

（2）若加密消息$P_i(1 \le i \le N)$，得到密文$C_i(1 \le i \le N)$。若加密者对消息P_k $(1 \le k < N)$进行了修改，则加密得到的密文 C_k 会发生变化，由于密文 C_k 反馈，所以 C_k 之后所有密文都会发生变化

（3）评分标准: 错一个扣 1 分,扣完为止（共 4 分）

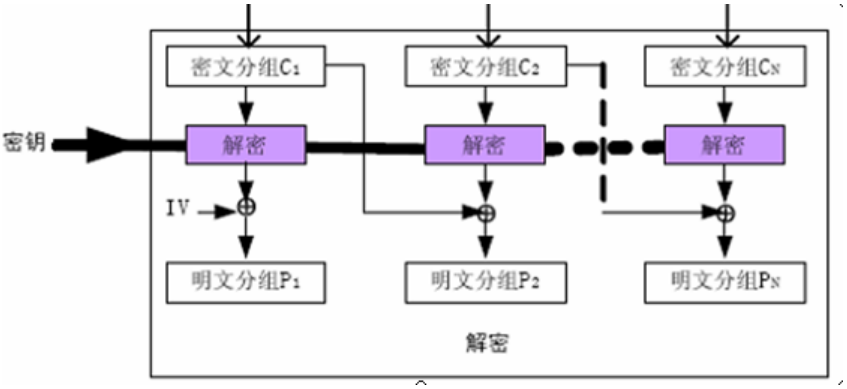


图 1 CBC 解密过程

20、序列密码考核

解： （1）

明文串对应的密钥流 $K = M \oplus C = 101000 \oplus 000110 = 101110$

（2）LFSR 反馈函数

3 级反馈函数表示为：$f(a_1\ a_2\ a_3) = c_1a_3 \oplus c_2a_2 \oplus c_3a_1$，根据已知密钥流可以得到下面三个方程

$$1 = c_1 \oplus c_3 \quad 1 = c_1 \oplus c_2 \quad 1 = c_1 \oplus c_2 \oplus c$$

因此得到 $c_1 = 0, c_2 = 1, c_3 = 1$，因此 $f(a_1\ a_2\ a_3) = a_2 \oplus a_1$

五、综合题

1、 Diffie-Hellman 密钥交换协议的考查 （18 分）

（1）求s_{A}，s_{B}，K 和K'的值

解：分别计算：$s_{\mathrm{A}} = a^{r_A} = 5^{11} mod\ 47 = 13$；

$s_{\mathrm{B}} = 5^{7} mod\ 47 = 11$；

在交换s_{A}，s_{B}后，

分别计算：$K = {s_B}^{r_A} mod\ 47 = 11^{11} mod\ 47 = 39$

$K' = {s_A}^{r_B} mod\ 47 = 13^{7} mod\ 47 = 39$

（2）解：基于离散对数困难问题，给定参数p, a，求s_A容易，反之，给定p和s_A，求a是困难的。参数s_B同理。

（3）通过中间人攻击，用户 A 计算共享密钥值为： $K = {s'_B}^{r_A} mod\ p$ 。用户 B 计算的共享密钥为：$K' = {s'_A}^{r_B} mod\ p$

2、AES 基本运算考查（12 分）

（4） 若用十六进制表示两域元素分别为{83}和{05}，则给出各域元素对应的多项式

解：83 对应的二进制为 10000011，对应的多项式为$x^7 + x + 1$。

05 对应的二进制为 00000101， 对应的多项式为$x^2 + 1$。

（5） 求两域元素的和：{83}+{05}

解：{83}+{05}=10000011⊕00000101=10000110={86}

（6） 求两域元素的积：{83}•{05}

解：

{83}•{05}={83}•{{04}⊕{01}} （1分）

{83}•{02}={10000011}•{02}={00000110}+{00011011}

={00011101}={1D} （2分）

{83}•{04}={1D}•{02}={00011101}•{02}={00111010}={3A} （2分）

{3A}+{83}={00111010}⊕{10000011}={10111001}={B9} （1分）

备注：也可以采用多项式直接求解

3. 在非对称密码算法 RSA 密钥产生过程中，设 p=13，q=17，取公钥参数 e＝25，完成（1）-（4）题。

（1） 求私钥参数 d；

φ(n)=12×16=192

192=25×7+17　　25=17+8　　17=8×2+1

1=17-8×2=17-(25-17)×2=17×3-25×2

=(192-25×7) ×3-25×2=192×3-25×23

等式两端模 192 得　　d≡-23≡169(mod 192)

（2） 如果消息 m=6，求对应的密文。

$6^2 \equiv 36 (mod 221)$　　$6^4 \equiv -30$　　$6^8 \equiv 16$

$6^{16} \equiv 256 \equiv 35$

$6^{25} \equiv 6 \times 6^8 \times 6^{16} \equiv 35 \times 16 \times 6 \equiv 45.$

（3）由上面结果，列出消息发送者和密码分析者各自可以直接获得的参数及对应的值。

消息发送者可以直接获得的参数及对应的值为：m=6, e=25, n=221, c=45

密码分析者可以直接获得的参数及对应的值为：e=25, n=221, c=45

（4） 简述 RSA 密码算法能否抵御选择明文攻击？

能

4. SHA

（1）W[0]=61316232H　　W[1]= 63336434H

W[2]=65358000H　W[15]= 00000050H

（2）$W[16] = ROTL^1(W[13] \oplus W[8] \oplus W[2] \oplus W[0])$

$=ROTL^1(61316232 \oplus 65358000)$

$=ROTL^1(404E232)= 809C464$

5 解: （1）请分别计算出 A 用户和 B 用户的私钥值 d 的值；

已知 公钥 n_A=65,首先分解 n_A=5*13 得到 p=5，q=13

计算欧拉函数 $\phi(n_A)$=（p-1）（q-1）=48

A 用户私钥计算：已知 A 用户私钥 d_A=7， gcd（$\phi(n_A)$，e_A）=1，根据 RSA 密钥生成过程 $e_Ad_A \equiv 1 \bmod \phi(n_A)$ 即 $7d_A \equiv 1 \bmod 48$

欧几里得扩展算法：48=6*7+6　7=6*1+1

1=7-6=7-(48-6*7)=7*7-48

可得 $7*7 \equiv 1 \bmod 48$ 即 d=7

同理 B 用户私钥：e_B=11，　$11d_B \equiv 1 \bmod 48$

48=4*11+4　11=2*4+3　4=1*3+1

1=4-(11-2*4)=3*4-11=3*(48-4*11)-11=3*48-13*11

d_B=48-13=35

（2）A 用户发送密文 C 和签名 Sig 给 B 用户

根据 RSA 加密算法规则，A 需要发送消息给 B，则需要用 B 的公钥加密

B 的公钥 e_B=11，因此密文 $C \equiv 2^{11} \bmod 65$

$C \equiv (2^{10})*2 \bmod 65 \equiv 49*2 \bmod 65 \equiv 33$

A 需要发送签名 Sig 给 B，则需要 A 的私钥签名，

A 的私钥 d_A=7， $Sig \equiv 2^7 \bmod 65 \equiv 63$

（3）

不安全

p 和 q 值太小，要求大素数 p 和 q,一般 1024bits 和 2048bits；

6、DH 算法（共 20 分）

解: （1）证明$K_A \equiv K_B$.

证明：

Q $y_A = g^{x_A} (\mathrm{mod}\ p), y_B = g^{x_B} (\mathrm{mod}\ p)$

$\therefore K_A \equiv y_B{}^{x_A} \equiv (g^{x_B})^{x_A} \equiv g^{x_B x_A} (\mathrm{mod}\ p)$

$\therefore K_B \equiv y_A{}^{x_B} \equiv (g^{x_A})^{x_B} \equiv g^{x_A x_B} (\mathrm{mod}\ p)$

$\therefore K_A \equiv K_B (\mathrm{mod}\ p)$

（2）求y_A，y_B，K_A.

Q $y_A \equiv g^{x_A} (\mathrm{mod}\ p) \equiv 5^{13} (\mathrm{mod}\, 97)$

$\equiv (5^3)^4 \cdot 5 (\mathrm{mod}\, 97) \equiv 28^4 \cdot 5 (\mathrm{mod}\, 97)$

$\equiv 8^2 \cdot 5 (\mathrm{mod}\, 97) \equiv 29 (\mathrm{mod}\, 97)$

$y_B = g^{x_B} (\mathrm{mod}\ p) \equiv 5^6 (\mathrm{mod}\, 97) \equiv 8$

$K_A \equiv y_A{}^{x_B} \equiv 29^6 (\mathrm{mod}\, 97) \equiv 65^3 (\mathrm{mod}\, 97)$

$\equiv 54 * 65 (\mathrm{mod}\, 97) \equiv 18 (\mathrm{mod}\, 97)$

（3） 在实际应用中，分析者可用直接获取p，g，y_A，y_B

（4）上面所述的 Diffie-Hellman 密钥交换协议有可能被中间人攻击。

第②步是 $y_C \equiv g^z (\mathrm{mod}\ p)$，第④步是 $y_C \equiv g^z (\mathrm{mod}\ p)$