1 填空题总结

1. 密码攻击的对象可以是加密算法, 也可以是密码协议. 对加密方案的攻击, 根据分析者使用的数据不同, 可以分为唯密文攻击、已知明文攻击、选择明文攻击、选择密文攻击. 其中破译难度最大的是选择密文攻击
2. 计算复杂性理论中, P-问题指一个问题已经找到了一个多项式算法, NP-问题指用非确定性算法 在多项式时间内 可以解决的算法, NPC-问题指用非确定性算法 不能在多项式时间 内解决的问题
3. IDEA 的明文和密文块都是64 比特, 密钥长度为128 比特, 加解密算法相同, 但密钥各异,
4. 密码体制的无条件保密性不能根据
5. 从密码系统角度看一个伪随机序列因该满足的条件是
   - [1] $\{a_i\}$ 的周期相当大
   - [2] $\{a_i\}$ 确定是计算上是容易的
   - [3] 由密文及相应明文的部分信息, 不能确定整个 $\{a_i\}$

2 简单题总结

1. 试简述计算复杂性理论在密码学中的作用

   在现代密码中, 一个密码系统的破译常常可以归结为求解某个数学问题, 数学问题的算法求解复杂性可通过计算复杂性理论来描述

   - [1] 计算复杂性理论位破译密码的计算复杂度提供了实际的度量方法
   - [2] 计算复杂性理论中的一些经典的数学问题给人们提供了设计实用安全的高强度密码系统的基础
2. 描述 FEAL 加密算法
   - [1] 1987 年两位日本学者在 DES 的基础上提出了一种快速数据加密算法 FEAL
   - [2] FEAl 的算法类似于 DES, 但其每轮都比 DES 强度大, 因为其轮次少, 运算速度比较快.

[3] 与 DES 的区别

- 增大了有效密钥的长度
- 减少了迭代次数
- 增强了加密函数 f 的复杂性
- 增强了密钥的控制作用

[4] FEAL 的整体结构

- 分组长度为 64 位
- 算法面向二进制设计
- 加密运算是对合运算
- $M \to$ 初始运算 $\to$ 四次迭代 $\to$ 末尾运算 $\to C$

3 计算题

1. 假设 Hill 密码使用密钥 $K = \begin{bmatrix} 11 & 8 \\ 3 & 7 \end{bmatrix}$, 试着对明文 regional 加密

   解: regional 对应明文数字序列 $M = (17, 4, 6, 8, 14, 13, 0, 11)$ 取 $l = 2, n = 26$ 密钥 $K = \begin{bmatrix} 11 & 8 \\ 3 & 7 \end{bmatrix}$

   于是有

   $$c_1 = 11 \times 17 + 8 \times 4 =$$
   $$c_2 = 3 \times 17 + 7 \times 4 =$$
   $$c_3 = 11 \times 6 + 8 \times 8 =$$
   $$c_4 = 3 \times 6 + 7 \times 8 =$$
   $$c_5 = 11 \times 14 + 8 \times 13 =$$
   $$c_6 = 3 \times 14 + 7 \times 13 =$$
   $$c_7 = 11 \times 0 + 8 \times 11 =$$
   $$c_8 = 3 \times 0 + 7 \times 11 =$$

2. 求解线性同余方程 $7x \equiv 23(\mathrm{mod} 41)$

   解: 因为 7 和 41 都是正整数, 且 41 为素数, $(7, 41) = 1$,

   所以 $7x \equiv 23(\mathrm{mod} 41)$ 有唯一解, $x \equiv a^{p-2}b(\mathrm{mod} p)$, 即 $x \equiv 7^{41-2} \times 23(\mathrm{mod} 41) \equiv 7^{39} \times 23(\mathrm{mod} 41)$

因为 $7^{\Phi(41)} = 7^{40} = 1(\text{mod}41)$

而 $7^{39} = 7^{40} \cdot 7^{-1} = 1 \cdot 7^{-1}(\text{mod}41) \equiv 7^{-1}(\text{mod}41) \equiv 6(\text{mod}41)$

所以 $x = 6 \times 23(\text{mod}41) \equiv 15(\text{mod}41)$

3. 求 $1004^{13}(\text{mod}2537)$

   解: 由题可知 $x = 1004, c = 23, n = 2537$

   $c = 13 = (1101)_2$

   $i = 3, c_3 = 1, z = z^2 \times x = 1^2 \times 1004 = 1004(\text{mod}2537)$

   $i = 2, c_2 = 1, z = z^2 \times x = 1004^2 \times 1004 = 709(\text{mod}2537)$

   $i = 1, c_1 = 0, z = z^2 = 709^2(\text{mod}2537) = 355(\text{mod}2537)$

   $i = 0, c_0 = 1, z = z^2 \times x = 355^2 \times 1004 = 1299(\text{mod}2537)$

4. 假设 $a = (2, 5, 9, 21, 45, 103, 215, 450)$ 是一个超递增序列, 取 $m' = 2003, w = 1531$. 试用背包密码对明文 $m = 11011010$ 加密

   解:

   (a) 计算公开钥由 $b_i \equiv wa_i(\text{mod}m')$

   $$b_1 = 1531 \times 2(\text{mod}2003) = 1059(\text{mod}2003)$$
   $$b_2 = 1531 \times 5(\text{mod}2003) = 1646(\text{mod}2003)$$
   $$b_3 = 1531 \times 9(\text{mod}2003) = 1761(\text{mod}2003)$$
   $$b_4 = 1531 \times 21(\text{mod}2003) = 103(\text{mod}2003)$$
   $$b_5 = 1531 \times 45(\text{mod}2003) = 793(\text{mod}2003)$$
   $$b_6 = 1531 \times 103(\text{mod}2003) = 1459(\text{mod}2003)$$
   $$b_7 = 1531 \times 215(\text{mod}2003) = 673(\text{mod}2003)$$
   $$b_8 = 1531 \times 450(\text{mod}2003) = 1921(\text{mod}2003)$$

   (b) 加密

   利用公式 $b = \sum_{i=1}^{n} b_i m_i$ 求得 b:

   $$b = 1059 + 1646 + 103 + 793 + 673 = 4274$$

   (c) 解密

[1] 利用欧几里得算法计算 w^{-1} 由 $ww^{-1} \equiv 1(\mathrm{mod} m')$ 及 $m' = 2003, w = 1531$ 得

$$w^{-1}1531 \equiv 1(\mathrm{mod}2003)$$
$$w^{-1} \equiv 1(\mathrm{mod}2003) = -836(\mathrm{mod}2003)$$

由 $a_i \equiv w^{-1}b_i(\mathrm{mod} m')$

5. 令 M=$\{a,b\}$, 有 $P(a) = \frac{1}{4}, P(b) = \frac{3}{4}, K = k_1, k_2, k_3$, 有 $P(k_1) = \frac{1}{2}, P(k_2) = \frac{1}{4}, P(k_3) = \frac{1}{4}, C = \{1,2,3,4\}$. 并假设加密函数定义如下: $E_{k_1}(a) = 1, E_{k_1}(b) = 2; E_{k_2}(b) = 1, E_{k_2}(b) = 3; E_{k_3}(a) = 2, E_{k_3}(b) = 4$, 计算该密码体制得熵

解: 这个密码体制可以通过下表表示

E_{k_1}	a	b
k_1	1	2
k_2	1	3
k_3	2	4

明文概率分布相关的熵为

$$\begin{aligned} H(M) &= -\sum_{m\in M} P(m)lbP(m) \\ &= -P(a)lbP(a) - P(b)lbP(b) \\ &= -\frac{1}{4}lb\frac{1}{4} - \frac{3}{4}lb\frac{3}{4} \\ &= -\frac{1}{4} \times (-2) - \frac{3}{4}(lb3 - 2) \qquad = 2 - \frac{3}{4}lb3 \approx 0.81 \end{aligned}$$

密钥概率分布相关的熵为

$$\begin{aligned} H(K) &= -\sum_{k\in K} P(k)lbP(k) \\ &= -P(k_1)lbP(k_1) - P(k_2)lbP(k_2) - P(k_3)lbP(k_3) \quad = 1.5 \end{aligned}$$

密文概率分布的熵为

$$H(C) = -\sum_{c\in C} P(c)lbP(c)$$

欲求出密文概率分布的熵, 首先要求出 $P(1), P(2), P(3), P(4)$

因为密钥 k 和明文 m 是相互独立的

所以

$$P(C)=\sum_{k\in K}\sum_{m\in M}P(m,k,c)$$

根据上表可得

$P(1)=P(b,k_1,1)+P(a,k_2,1)=P(b)\cdot P(k_1)+P(a)\cdot P(k_2)=\frac{1}{4}\times\frac{1}{4}+\frac{3}{4}\times\frac{1}{2}=\frac{7}{16}$

$P(2)=P(b,k_1,2)+P(a,k_3,2)=P(b)\cdot P(k_1)+P(a)\cdot P(k_3)=\frac{1}{4}\times\frac{1}{4}+\frac{3}{4}\times\frac{1}{2}=\frac{7}{16}$

$P(3)=P(b,k_2,3)=P(b)\cdot P(k_2)=\frac{1}{4}\times\frac{1}{4}=\frac{7}{16}$

$P(4)=P(b,k_3,4)=P(b)\cdot P(k_3)=\frac{1}{4}\times\frac{1}{4}=\frac{7}{16}$

6. 画出以 $f(x)=x^5+x^3+x+1$ 表示 5 级 LFSR 的循环结构, 若初始状态为 01101, 是求出其输出序列及其周期

解: 由题可知 $C_1=1, C_2=0, C_3=1, C_4=0, C_5=1$

则有 $\begin{aligned}f(a_1,a_2,a_3,a_4,a_5)&=C_5a_1\oplus C_4a_2\oplus C_3a_3\oplus C_2a_4\oplus C_1a_5\\&=a_1\oplus a_3\oplus a_5\end{aligned}$

$S_1=(a_1,a_2,a_3,a_4,a_5)=(01101)_2,$输出为$a_1=0$

$a_6=a_1\oplus a_3\oplus a_5=0\oplus 1\oplus 1=0, S_2=(a_2,a_3,a_4,a_5,a_6)=(11010),$输出为$a_2=1$

$a_7=a_2\oplus a_4\oplus a_6=1\oplus 0\oplus 0=1, S_3=(a_2,a_3,a_4,a_5,a_6)=(10101),$输出为$a_3=1$

$a_8=a_3\oplus a_5\oplus a_7=1\oplus 1\oplus 1=1, S_4=(a_3,a_4,a_5,a_6,a_7)=(01011),$输出为$a_4=0$

$a_9=a_4\oplus a_6\oplus a_8=0\oplus 0\oplus 1=1, S_5=(a_4,a_5,a_6,a_7,a_8)=(10111),$输出为$a_5=1$

$a_{10}=a_5\oplus a_7\oplus a_9=1\oplus 1\oplus 1=1, S_6=(a_5,a_6,a_7,a_8,a_9)=(01111),$输出为$a_6=0$

$a_{11}=a_6\oplus a_8\oplus a_{10}=0\oplus 1\oplus 1=0, S_7=(a_6,a_7,a_8,a_9,a_10)=(11110),$输出为$a_7=1$

$a_{12}=a_7\oplus a_9\oplus a_{11}=1\oplus 1\oplus 0=0, S_8=(a_7,a_8,a_9,a_10,a_11)=(11100),$输出为$a_8=1$

$a_{13}=a_8\oplus a_{10}\oplus a_{12}=1\oplus 1\oplus 0=0, S_9=(a_8,a_9,a_10,a_11,a_12)=(11000),$输出为$a_9=1$

$a_{14}=a_9\oplus a_{11}\oplus a_{13}=1\oplus 0\oplus 0=1, S_{10}=(a_9,a_{10},a_{11},a_{12},a_{13})=(10001),$输出为$a_{10}=1$

$a_{15}=a_{10}\oplus a_{12}\oplus a_{14}=1\oplus 0\oplus 1=0, S_{11}=(a_{10},a_{11},a_{12},a_{13},a_{14})=(00010),$输出为$a_{11}=0$

$a_{16}=a_{11}\oplus a_{13}\oplus a_{15}=0\oplus 0\oplus 0=0, S_{12}=(a_{11},a_{12},a_{13},a_{14},a_{15})=(00100),$输出为$a_{12}=0$

$a_{17}=a_{12}\oplus a_{14}\oplus a_{16}=0\oplus 1\oplus 0=1, S_{13}=(a_{12},a_{13},a_{14},a_{15},a_{16})=(01001),$输出为$a_{13}=0$

输出序列为 011010111100010011010111110 $\cdots$ 以 15 为周期

7. 假设 $p = 83, q = 41, h = 2$

   (a) 求参数 g

   $$p = 83 = 2q + 1$$
   $$g \equiv 2^2(\bmod 83) = 4(\bmod 83)$$

   (b) 取私钥 $x = 57$, 求公钥 y

   $$y \equiv g^x(\bmod p) \equiv 4^{57}(\bmod 83) = 77(\bmod 83)$$

   (c) 明文 $m = 56$, 取随机数 $k = 23$, 求 m 的签名因为 $k^{-1}k \equiv 1(\bmod q)$

   所以

   $k^{-1} = -16$

   $r = [g^k(\bmod p)](\bmod q) = [4^{23}(\bmod 83)](\bmod 41) = 10$

   $s = [k^{-1}(H(m) + xr)](\bmod q) = [-16 \times (56 + 57 \times 10)](\bmod 41) = 29$

   于是消息 56 的签名为 (10, 29)

8. 已知放射变换为 $c = 11m + 7(\bmod 26)$, 试对明文 matrix 加密.

   解: 明文 matrix 对应的序列为 (12,0,19,17,8,23)

   $c_1 = 11m_1 + 7(\bmod 26) = 11 \times 12 + 7(\bmod 26) = 9(\bmod 26)$

   $c_2 = 11m_2 + 7(\bmod 26) = 11 \times 0 + 7(\bmod 26) = 7(\bmod 26)$

   $c_3 = 11m_3 + 7(\bmod 26) = 11 \times 19 + 7(\bmod 26) = 8(\bmod 26)$

   $c_4 = 11m_4 + 7(\bmod 26) = 11 \times 17 + 7(\bmod 26) = 12(\bmod 26)$

   $c_5 = 11m_5 + 7(\bmod 26) = 11 \times 8 + 7(\bmod 26) = 17(\bmod 26)$

   $c_6 = 11m_6 + 7(\bmod 26) = 11 \times 23 + 7(\bmod 26) = 0(\bmod 26)$

   故密文序列为 (9,7,8,12,17,0), 对应密文为 jhimra

9. 假设 Hill 密码使用密钥 $K = \begin{bmatrix} 8 & 6 & 9 & 5 \\ 6 & 9 & 5 & 10 \\ 5 & 8 & 4 & 9 \\ 10 & 6 & 11 & 4 \end{bmatrix}$, 试对明文 best 加密

解: 明文 best 对应序列为 (1, 4, 18, 19), $l=4, n=26$

$$
\begin{aligned}
c_1 &= 8\times1+6\times4+9\times18+5\times19(\mathrm{mod}26)= \\
c_2 &= 6\times1+9\times4+5\times18+10\times19(\mathrm{mod}26)= \\
c_3 &= 5\times1+8\times4+4\times18+9\times19(\mathrm{mod}26)= \\
c_4 &= 10\times1+6\times4+11\times18+4\times19(\mathrm{mod}26)=
\end{aligned}
$$

10. 使用欧几里得算法求 47(mod211) 的逆元.

解: 设 47 的逆元为 w^{-1}, 则 $w^{-1}47=1(\mathrm{mod}211)$ 首先辗转相除法

$$
\begin{aligned}
1 &= 47-46 \\
&= 47-2\times23 \\
&= 47-2\times(211-4\times47) \\
&= 9\times49-2\times211
\end{aligned}
$$

所以逆元为 9(mod211)

11. 考虑一个密码体制 $M=\{a,b,c\}, K=\{k_1,k_2\}, C=\{1,2,3,4\}$,

假设加密矩阵为

	a	b	c
k_1	2	3	4
k_2	3	4	1

已知密钥的概率分布 $P(k_1)\frac{1}{4}, P(k_2)=\frac{3}{4}$, 明文概率分布为 $P(a)=\frac{1}{4}, P(b)=\frac{1}{4}, P(c)=\frac{1}{2}$. 计算 $H(M), H(K), H(C)$

解: 由公式 $H(M)=-\sum\limits_{m\in M}P(m)lbP(m)$ 得

$$
\begin{aligned}
H(M) &= -P(a)lbP(a)-P(b)lbP(b)-P(c)lbP(c) \\
&= -\frac{1}{4}lb\frac{1}{4}-\frac{3}{4}lb\frac{3}{4}-\frac{1}{2}lb\frac{1}{2} \\
&= -\frac{1}{4}\times(-2)-\frac{1}{4}\times(-2)-\frac{1}{2}\times(-1) \\
&\approx 1.5
\end{aligned}
$$

由公式 $H(K) = -\sum_{k \in K} P(k) lbP(k)$ 得

$$\begin{aligned} H(K) &= -P(k_1)lbP(k_1) - P(k_2)lbP(k_2) \\ &= -\frac{1}{4}lb\frac{1}{4} - \frac{3}{4}lb\frac{3}{4} - \frac{1}{2}lb\frac{1}{2} \\ &= -\frac{1}{4} \times (-2) - \frac{3}{4} \times (lb3 - 2) \\ &\approx 0.81 \end{aligned}$$

由公式 $H(C) = -\sum_{c \in C} P(c) lbP(c)$

可知要求 $H(C)$, 首先要求出 $P(C)$

由公式 $P(C) = \sum_{m \in M} \sum_{k \in K} P(m, k, c)$

由上表可知

$P(1) = P(c, k_2, 1) = P(c)P(k_2) = \frac{1}{2} \times \frac{3}{4} = \frac{3}{8}$

$P(2) = P(a, k_1, 2) = P(a)P(k_1) = \frac{1}{4} \times \frac{1}{4} = \frac{1}{16}$

$P(3) = P(b, k_1, 3) + P(a, k_2, 3) = P(b)P(k_1) + P(a)P(k_2) = \frac{1}{4} \times \frac{1}{4} + \frac{1}{4} \times \frac{3}{4} = \frac{1}{4}$

$P(4) = P(c, k_1, 4) = P(c)P(k_1) = \frac{1}{2} \times \frac{1}{4} = \frac{1}{8}$

得

$$\begin{aligned} H(M) &= -P(1)lbP(1) - P(2)lbP(2) - P(3)lbP(3) - P(4)lbP(4) \\ &= -\frac{1}{4}lb\frac{1}{4} - \frac{3}{4}lb\frac{3}{4} - \frac{1}{2}lb\frac{1}{2} \\ &= -\frac{1}{4} \times (-2) - \frac{3}{4} \times (lb3 - 2) \\ &\approx 0.81 \end{aligned}$$

12. 求解线性同余方程 $5x \equiv 19(\text{mod}31)$

由题可知 (5, 31)=1, 所以该方程有唯一解

由公式 $x \equiv a^{p-2}b(\text{mod}p)$ 得 $x \equiv 5^{31-2} \times 19(\text{mod}31) \equiv 5^{29} \times 19(\text{mod}\ 31)$

因为 $5^{\Phi(31)} = 5^{30} \equiv 1(\text{mod}31)$

所以 $5^{29} \equiv 5^{-1} \times 5^{30} (\mathrm{mod} 31) \equiv 5^{-1} (\mathrm{mod} 31)$

由欧几里得算法可得 $5^{-1} (\mathrm{mod} 31) \equiv (-6) (\mathrm{mod} 31)$

所以 $x \equiv 19 \times (-6) (\mathrm{mod} 31) \equiv 10 (\mathrm{mod} 31)$

13. 求 $1004^{13} (\mathrm{mod} 2537)$

解: 由题得 $x = 1004, c = 13, n = 2537$

$c = 13 = (1101)_2, z = 1$

$i = 3, c_3 = 1, z = z^2 \times x (\mathrm{mod} n) = 1004 (\mathrm{mod} 2537)$

$i = 2, c_2 = 1, z = z^2 \times x (\mathrm{mod} n) = 1004^2 \times 1004 (\mathrm{mod} 2537) = 709 (\mathrm{mod} 2537)$

$i = 1, c_1 = 0, z = z^2 (\mathrm{mod} n) = 709^2 (\mathrm{mod} 2537) = 355 (\mathrm{mod} 2537)$

$i = 0, c_0 = 1, z = z^2 \times x (\mathrm{mod} n) = 355^2 \times 1004 (\mathrm{mod} 2537) = 1299 (\mathrm{mod} 2537)$

解: 假设 $a = (2, 5, 9, 21, 45, 103, 215, 450)$ 是一个超递增序列, 取 $m' = 2007, w = 1531$, 用背包加密算法对明文 $m = 10011011$ 加密

解: 首先利用公式 $b_i = wa_i (\mathrm{mod} m')$

$$b_1 = wa_1 (\mathrm{mod} m') = 1531 \times 2 (\mathrm{mod} 2007) = 1055 (\mathrm{mod} 2007)$$
$$b_2 = wa_2 (\mathrm{mod} m') = 1531 \times 5 (\mathrm{mod} 2007) = 1634 (\mathrm{mod} 2007)$$
$$b_3 = wa_3 (\mathrm{mod} m') = 1531 \times 9 (\mathrm{mod} 2007) = 1737 (\mathrm{mod} 2007)$$
$$b_4 = wa_4 (\mathrm{mod} m') = 1531 \times 21 (\mathrm{mod} 2007) = 39 (\mathrm{mod} 2007)$$
$$b_5 = wa_5 (\mathrm{mod} m') = 1531 \times 45 (\mathrm{mod} 2007) = 657 (\mathrm{mod} 2007)$$
$$b_6 = wa_6 (\mathrm{mod} m') = 1531 \times 103 (\mathrm{mod} 2007) = 1147 (\mathrm{mod} 2007)$$
$$b_7 = wa_7 (\mathrm{mod} m') = 1531 \times 215 (\mathrm{mod} 2007) = 17 (\mathrm{mod} 2007)$$
$$b_8 = wa_8 (\mathrm{mod} m') = 1531 \times 450 (\mathrm{mod} 2007) = 549 (\mathrm{mod} 2007)$$

然后利用公式 $b = \sum_{i=1}^{n} b_i m_i$ 求得 $b = 1055 + 39 + 657 + 17 + 549 = 2317$

即密文为 2317

4 J-K 触发器专题

J-K 触发器可以用以下递推公式计算

$$c_n = ((a_n + b_n + 1) \times c_{n-1} + a_n) \bmod 2$$

表 1: J-K 触发器真值表

J	K	C_K
0	0	C_{K-1}
0	1	0
1	0	1
1	1	$\overline{C_{K-1}}$

4.1 例题

已知 LFSR1 生成周期为 3 的序列

$$\{a_k\} = 0, 1, 1, \cdots$$

LFSR2 生成周期为 4 的序列

$$\{b_k\} = 1, 0, 0, 1 \cdots$$

结合上表可得

$$J = a_1 = 0, K = b_1 = 1, c_1 = 0$$
$$J = a_2 = 1, K = b_2 = 0, c_2 = 1$$
$$J = a_3 = 1, K = b_3 = 0, c_3 = 1$$
$$J = a_4 = 0, K = b_4 = 1, c_4 = 0$$
$$J = a_5 = 1, K = b_5 = 1, c_5 = 1$$
$$J = a_6 = 1, K = b_6 = 0, c_6 = 1$$
$$J = a_7 = 0, K = b_7 = 0, c_7 = 1$$
$$J = a_8 = 1, K = b_8 = 1, c_8 = 0$$
$$J = a_9 = 1, K = b_9 = 1, c_9 = 1$$
$$J = a_{10} = 0, K = b_{10} = 0, c_{10} = 1$$
$$J = a_{11} = 1, K = b_{11} = 0, c_{11} = 1$$
$$J = a_{12} = 1, K = b_{12} = 1, c_{12} = 0$$

生成序列为 $011011101110\cdots$, 周期为 12

5 传统密码专题

[1] 已知仿射变换为 $c = 5m + 7 (\mathrm{mod} 26)$, 试对密文 VMWZ 解密

解: VMWZ 对应的序列为 $(21, 12, 22, 25)$ 由题可知 $m = 5^{-1} \times (c - 7)(\mathrm{mod} 26)$ 因为 $5^{-1}(\mathrm{mod} 26) = (-5)(\mathrm{mod} 26)$

所以 $m = (-5) \times (c - 7)(\mathrm{mod} 26)$

所以

$$m_1 = (-5) \times (c_1 - 7)(\mathrm{mod} 26) = (-5) \times 14 (\mathrm{mod} 26) = 8 (\mathrm{mod} 26)$$
$$m_2 = (-5) \times (c_2 - 7)(\mathrm{mod} 26) = (-5) \times 5 (\mathrm{mod} 26) = 1 (\mathrm{mod} 26)$$
$$m_3 = (-5) \times (c_3 - 7)(\mathrm{mod} 26) = (-5) \times 15 (\mathrm{mod} 26) = 3 (\mathrm{mod} 26)$$
$$m_4 = (-5) \times (c_4 - 7)(\mathrm{mod} 26) = (-5) \times 18 (\mathrm{mod} 26) = 14 (\mathrm{mod} 26)$$

密文为 ibdo

[2] 假设明文 friday 利用 $l = 2$ 的 Hill 密码加密, 得到密文 PQCFKU, 试求密钥 K

解: 明文 friday 对应的序列为 $[5, 17, 8, 3, 0, 24]$

密文 PQCFKU 对应的序列为 $[15, 16, 2, 5, 10, 20]$

由于 $l = 2$ 可得

$$\begin{bmatrix} 15 \\ 16 \end{bmatrix} = K \begin{bmatrix} 5 \\ 17 \end{bmatrix} (\bmod 26)$$

$$\begin{bmatrix} 2 \\ 5 \end{bmatrix} = K \begin{bmatrix} 8 \\ 3 \end{bmatrix} (\bmod 26)$$

$$\begin{bmatrix} 10 \\ 20 \end{bmatrix} = K \begin{bmatrix} 0 \\ 24 \end{bmatrix} (\bmod 26)$$

联立前两个方程得

$$\begin{bmatrix} 15 & 2 \\ 16 & 5 \end{bmatrix} = K \begin{bmatrix} 5 & 8 \\ 17 & 3 \end{bmatrix} (\bmod 26)$$

因为 $\begin{vmatrix} 15 & 2 \\ 16 & 5 \end{vmatrix} = 43, (43, 26) = 1, (-3) \times 43 (\bmod 26) \equiv 1 (\bmod 26)$

所以 $(detA)^{-1} = -3$

容易算出

$$\begin{aligned} \begin{bmatrix} 15 & 2 \\ 16 & 5 \end{bmatrix}^{-1} &= (-3) \begin{bmatrix} 15 & 2 \\ 16 & 5 \end{bmatrix} \\ &= \begin{bmatrix} -15 & 6 \\ 48 & -75 \end{bmatrix} (\bmod 26) \\ &= \begin{bmatrix} 11 & 6 \\ 22 & 3 \end{bmatrix} (\bmod 26) \end{aligned}$$

所以

$$\begin{aligned} K &= \begin{bmatrix} 5 & 8 \\ 17 & 3 \end{bmatrix} \begin{bmatrix} 11 & 6 \\ 22 & 3 \end{bmatrix} (\bmod 26) \\ &= \begin{bmatrix} 231 & 54 \\ 253 & 111 \end{bmatrix} (\bmod 26) \\ &= \begin{bmatrix} 23 & 2 \\ 19 & 7 \end{bmatrix} (\bmod 26) \end{aligned}$$

6 分组密码

[1] 设 DES 数据加密标准中已知明文 m, 和密钥 k, 试求 L_1 和 R_1

(a) IP 置换, 得到置换后的明文 (64 位), 一分为二得到 L_0, R_0

(b) PC-1 置换, 得到置换后的密钥 (56 位), 一分为二得到 $C_0, D_0(56 \to$ 28 位)

(c) 循环左移, 参照循环左移表, 得到 $C_0 \sim C_{16}, D_0 \sim D_{16}$(28 位)

(d) PC-2 置换, 将 C_i 和 D_i 结合起来, 再进行 PC-2 置换, 得到 K_i(48 位)

(e) E 置换, 针对于 R_i, 将 32 位置换为 48 位.

(f) $E(R_{i-1}) \oplus K_i$: 将上面两步产生的 R_{i-1} 和 K_i 相 $\oplus$(48 位)

(g) S 盒输出, 将上一步产生的序列平均分为 8 组, 每组 6 比特, 经过 S 盒置换后, 每组得到 4 比特, 总共 32 比特

(h) P 置换, 得到加密函数 $f(R_{i-1}, K_i)$

(i) $R_i = L_{i-1} \oplus f(R_{i-1}, K_i)$

[2] 已知 IDEA 密码算法中

$$Z_1^{(1)} = 1000010010011101 = 33949$$

求 $[Z_1^{(1)}]^{-1}$ 与 $-Z_1^{(1)}$

由 $Z \odot Z^{-1} \equiv 1(\text{mod} 2^{16}+1)$ 即

7 公钥密码

[1] 求解下列同余方程组

$$\begin{cases} x \equiv 2(\text{mod} 3) \\ x \equiv 1(\text{mod} 5) \\ x \equiv 1(\text{mod} 7) \end{cases}$$

由题可知 $b_1 = 2, b_2 = 1, b_3 = 1, m_1 = 3, m_2 = 5, m_5 = 7$

则

$$
\begin{aligned}
M &= m_1m_2m_3 = 3\times 5\times 7 = 105\\
M_1 &= m_2m_3 = 5\times 7 = 35\\
M_2 &= m_1m_3 = 3\times 7 = 21\\
M_3 &= m_1m_2 = 3\times 5 = 15
\end{aligned}
$$

所以

$$
\begin{cases}
35y_1 = 1(\bmod 3), y_1 = 2\\
21y_2 = 1(\bmod 5), y_2 = 1\\
15y_3 = 1(\bmod 7), y_3 = 1
\end{cases}
$$

所以

$$
\begin{aligned}
x &\equiv b_1M_1y_1 + b_2M_2y_2 + b_3M_3y_3(\bmod 105)\\
&\equiv 2\times 35\times 2 + 1\times 21\times 1 + 1\times 15\times 1\\
&\equiv 176(\bmod 105)\\
&\equiv 71(\bmod 105)
\end{aligned}
$$