作业二

(密码学与网络安全课程报告)

姓 名： 肖文韬

学 号： 2020214245

专 业 方 向： 电子信息（计算机技术）

邮 箱： xwt20@mails.tsinghua.edu.cn

二〇二一年三月七日

第 1 章　作业内容

1. 考虑一个密码体系 $M = \{a, b, c\}, K = \{k_1, k_2, k_3\}$ 和 $C = \{1, 2, 3, 4\}$, 将明文 M 使用密钥 K 加密为密文 C。假设加密矩阵如下表。

	a	b	c
k_1	2	3	4
k_2	3	4	1
k_3	1	2	3

已知密钥概率分布 $p(k_3) = 1/2, p(k_2) = p(k_1) = 1/4$, 且明文概率分布 $p(a) = 1/3, p(b) = 8/15, p(c) = 2/15$。请计算 $H(M), H(K), H(C), H(M|C), H(K|C)$。

解:

$$H(M) = \sum_i p(M_i)I(M_i) = -\sum_i p(M_i)\log p(M_i) \approx 1.3996 \tag{1-1}$$

$$H(K) \approx 1.5 \tag{1-2}$$

$$H(C) \approx 1.9408 \quad (p(C) = [0.2, 0.35, 0.2833, 0.1667]) \tag{1-3}$$

$$\begin{aligned} H(M|C) &= H(MC) - H(C) \\ &= -\sum_i \sum_j p(M_i, C_j)\log p(M_i, C_j) \approx 2.8996 \end{aligned} \tag{1-4}$$

$$H(K|C) = H(KC) - H(C) \approx 2.8996 \tag{1-5}$$

2. 计算英文字母的凯撒密码的唯一解距离。

解:

$N = H(K)/D = -\log(1/26)/3.2 \approx 2$

3. 计算重复周期为 6 的维吉尼亚密码的唯一解距离。

解:

$N = H(K)/D = -\log(\frac{1}{26^6})/3.2 \approx 9$

4. 某次 AES 加密的轮函数过程中，字节替代的结果为:

$$A=\begin{bmatrix}87 & F2 & 4D & 97\\ EC & 6E & 4C & 90\\ 4A & C3 & 46 & E7\\ 8C & D8 & 95 & A6\end{bmatrix} \tag{1-6}$$

解:

求这个矩阵经过行移位变换后的结果, 以及经过列混淆后第三行第一列的值。

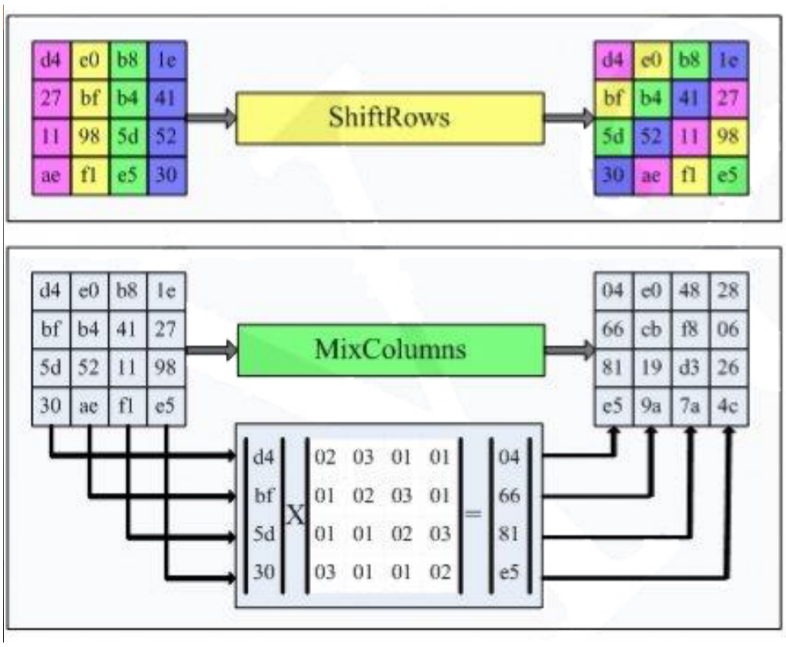

图 1.1　移位变换和列混淆的具体过程

移位变换和列混淆的具体过程如图 1.1所示。移位表换后的结果为 B.

$$B=\begin{bmatrix}87 & F2 & 4D & 97\\ 6E & 4C & 90 & EC\\ 46 & E7 & 4A & C3\\ A6 & 8C & D8 & 95\end{bmatrix} \tag{1-7}$$

列混淆后的结果为 C.

$$C = \begin{bmatrix} 47 & 40 & A3 & 4C \\ 37 & D4 & 70 & 9F \\ 94 & E4 & 3A & 42 \\ ED & A5 & A6 & BC \end{bmatrix} \tag{1-8}$$

5. 思考题：为何 AES 加密算法的最后一轮与前 9 轮不同?

解：

AES 算法在处理的轮数上只有最后一轮与前面 9 轮不同之处在于最后一轮少了列混淆处理。理由:

在正常的 AES 轮中，列混淆会在轮密钥加操作之前进行。不过，也可以调换这些操作的顺序。先执行轮密钥加操作，再执行列混淆操作，稍加修改，就可以收到同样的结果。因此，可以认为最后的列混淆不会增加任何安全性, 因为它是一个不加键、可逆的操作, 可以使其成为最后一轮的最后一步。

然而理论上我们可以进行攻击。考虑到一个 AES 变体，其中列混淆在最后一轮加密中执行。为了攻击解密函数，攻击者可能会交换列混淆和轮密钥加的顺序，这样他就可以直接撤销列混淆。现在假设他能够（以某种方式）恢复轮密钥加中使用的轮密钥的一些信息。因为他交换了操作，所以他恢复的实际上并不是键表（Key schedule）吐出的轮密钥的信息，而是应用了逆列混淆的轮密钥的信息。