信息安全 作业1

> 姓名：TRY
>
> 学号：
>
> 专业：计算机科学与技术

本次作业，选择第1、2、3、5、6题进行练习。

Problem 1

- 题目：

  Problem 1　Vigenère Cipher. Suppose you have a language with only the 3 letters A, B, C, and they occur with frequencies 0.7, 0.2, and 0.1. The following ciphertext was encrypted by the Vigenère cipher:

  $$ABCBABBBAC.$$

  Suppose you are told that the key length is 1, 2, or 3. Show that the key length is probably 2, and determine the most probable key.

- 在原密文"**AB**CB**AB**BBAC"中，可以发现有2个相同的密文“AB”，它们之间的距离为4。因此，可以猜测，密钥长度为距离4的因子，故“密钥长度=3”可以被排除。此时，**分类讨论** “密钥长度=1或2”：

- **当密钥长度为2时**，原密文可以划分如下：

  $$AB|CB|AB|BB|AC$$

  可以发现，在**第2个位置**中，出现了4个“`B`”，而由题可知，在明文中，$A:B:C=7:2:1$，而在密文中正好有10个字母，所以，为了满足频率要求，上面所说的“`B`”对应明文中的“`A`”。（10个字母中，只有A超过了4，所以对应A）所以，第二个位置的密钥为1。

  现考虑**第1个位置**，发现密文中的$A:B:C=3:1:1$，而明文中剩余的字母频率比为$A:B:C=3:1:1$，因此可知第一个密钥为0时，满足频率比。

  故可能的密钥为（0,1），且此时最符合频率比。

- **当密钥长度为1时**，原密文可以划分如下：

  $$A|B|C|B|A|B|B|B|A|C$$

  此时密文中的$A:B:C=3:5:2$，不可能解密成7 : 2 : 1的比例。因此，密钥长度为1不满足题意。

- **综上所述，密钥长度最可能为2，且密钥为（0,1）。**

Problem 2

- 题目：

Problem 2 **Perfect secrecy and one-time-pad.**

1. For a perfect secret encryption scheme $E(K, M) = C$, prove: $\Pr[C = c|M = m] = \Pr[C = c]$.
2. Consider a biased one-time-pad system, where $\Pr[M = b] = p_b$, $b = 0, 1$ and $\Pr[K = 0] = 0.4$. The first attacker Randy randomly guesses $M = 1$ or $M = 1$: prove that the probability of success is 0.5. The second attacker Smarty guesses M based on C and p_0, p_0: suggest a good attack strategy.

1. For a perfect secret encryption scheme `E(K, M)=C`, prove: `Pr[C = c|M = m] = Pr[C = c]`

- 对于一个 **"perfect secret完全安全"** 的密码系统，有

$$Pr[M = m|C = c] = Pr[M = m]$$

由条件概率公式可得:

$$Pr[M = m|C = c] = \frac{Pr[M = m, C = c]}{Pr[C = c]}$$

所以，由上面2式可得:

$$Pr[M = m, C = c] = Pr[M = m]Pr[C = c]$$

变形，有

$$Pr[C = c] = \frac{Pr[M = m, C = c]}{Pr[M = m]}$$

由条件概率定义，有

$$Pr[C = c] = Pr[C = c|M = m]$$

证毕。

2. Consider a biased one-time-pad system, where `Pr[M = b]` = p_b, `b` = 0, 1 and `Pr[K = 0] = 0.4`.

(1) The first attacker Randy randomly guesses M = 1 or M = 0: prove that the probability of success is 0.5.

- 设攻击者猜测`M`=1的概率为 p'，猜测`M`=0的概率为 p''。
- 由题可知，攻击者是随机猜测的，所以 $p' = p'' = 0.5$
- 因此，攻击者猜测正确的概率为

$$p_{correct} = p_0 * p' + p_1 * p'' = 0.5 * (p_0 + p_1)$$

而已知`b` 取0,1，所以 $p_0 + p_1 = 1$

故

$$p_{correct} = 0.5 * 1 = 0.5$$

(2) The second attacker Smarty guesses M based on C and p0, p1: suggest a good attack strategy.

- 首先，我们知道明文取0或1这一事件和密钥取0或1这一事件是**相互独立**的（明文和密钥的取值无直接关系），所以有

$$\begin{aligned}
p(M = 0, k = 0) = p(M = 0) * p(k = 0) = p_0 * 0.4 = 0.4p_0 \\
p(M = 1, k = 0) = p(M = 1) * p(k = 0) = p_1 * 0.4 = 0.4p_1 \\
p(M = 0, k = 1) = p(M = 0) * p(k = 1) = p_0 * (1 - 0.4) = 0.6p_0 \\
p(M = 1, k = 1) = p(M = 1) * p(k = 1) = p_1 * (1 - 0.4) = 0.6p_1
\end{aligned}$$

- 所以，由one-time-pad的**异或**操作可知，可以得到取对应密文的概率以及明文和密文取值的联合概率：

$$p(C=1)=p(M=1,k=0)+p(M=0,k=1)=0.4p_1+0.6p_0$$
$$p(C=0)=p(M=0,k=0)+p(M=1,k=1)=0.4p_0+0.6p_1$$
$$p(M=1,C=1)=0.4p_1$$
$$p(M=1,C=0)=0.6p_1$$
$$p(M=0,C=1)=0.6p_0$$
$$p(M=0,C=0)=0.4p_0$$

- 所以，得到明文密文取值的条件概率：

$$p(M=1|C=1)=\frac{p(M=1,C=1)}{p(C=1)}=\frac{0.4p_1}{0.4p_1+0.6p_0}$$
$$p(M=0|C=1)=\frac{p(M=0,C=1)}{p(C=1)}=\frac{0.6p_0}{0.4p_1+0.6p_0}$$
$$p(M=1|C=0)=\frac{p(M=1,C=0)}{p(C=0)}=\frac{0.6p_1}{0.4p_0+0.6p_1}$$
$$p(M=0|C=0)=\frac{p(M=0,C=0)}{p(C=0)}=\frac{0.4p_0}{0.4p_0+0.6p_1}$$

- 由上式可知，当$C=1$时，若$p(M=1|C=1)>p(M=0|C=1)$，即$p_1>\frac{3}{2}p_0$时，猜测$M=1$；当$p_1\leq\frac{3}{2}p_0$时，猜测$M=0$。同理，当$C=0$时，若$p_1>\frac{2}{3}p_0$时，猜测$M=1$；当$p1\leq\frac{2}{3}p_0$时，猜测$M=0$.
- 综上所述，当 C , p_0和 p_1满足下面的条件时，可以做出对应的猜测：

$$guess\ M=\begin{cases}1, & when\ (p_1>\frac{3}{2}p_0)\ or\ (C=0\ and\ \frac{2}{3}p_0<p_1\leq\frac{3}{2}p_0)\\ 0, & when\ (0\leq p_1\leq\frac{2}{3}p_0)\ or\ (C=1\ and\ \frac{2}{3}p_0<p_1\leq\frac{3}{2}p_0)\end{cases}$$

Problem 3

- 题目：

Problem 3 **DES**. Before 2-DES and 3-DES was invented, the researchers at RSA Labs came up with DESV and DESW, defined by

$$DESV_{kk_1}(M)=DES_k(M)\oplus k_1,\ DESW_{kk_1}(M)=DES_k(M\oplus k_1).$$

In both schemes, $|k|=56$ and $|k_1|=64$. Show that both these proposals do not increase the work needed to break them using brute-force key search. That is, show how to break these schemes using on the order of 2^{56} DES operations. You have a small number of plaintext-ciphertext pairs.

- 为了**破解DESV**，可以设2对不同的明文-密文对，$<M_1,C_1>,<M_2,C_2>$，有：

$$C_1=DES_k(M_1)\oplus k_1$$
$$C_2=DES_k(M_2)\oplus k_1$$

然后，将上面2式进行异或操作，得：

$$\begin{aligned}C_1\oplus C_2&=[DES_k(M_1)\oplus k_1]\oplus[DES_k(M_2)\oplus k_1]\\&=DES_k(M_1)\oplus DES_k(M_2)\end{aligned}$$

而 C_1,C_2,M_1,M_2 都是已知的，因此可以用**暴力法**，遍历 `k` 来寻找合适的 `k` 满足 $C_1\oplus C_2=DES_k(M_1)\oplus DES_k(M_2)$，这需要 $M_1 2^{56}$和$M_2 2^{56}$的时间，即复杂度为$O(2^{56})$ 。

而解密 `k1`，只需要在找到 `k` 的基础上，通过下式解出 `k1`：

$$k_1=C_1\oplus DES_k(M_1)$$

因此，总共需要2^{56} 的DES操作来破解DESV。

- 为了**破解DESW**，可以同样设2对不同的明文-密文对，$< M_1, C_1 >, < M_2, C_2 >$，有：

$$DES_k^{-1}(C_1) = M_1 \oplus k_1$$
$$DES_k^{-1}(C_2) = M_2 \oplus k_1$$

然后，将上面2式进行异或操作，得：

$$\begin{aligned} DES_k^{-1}(C_1) \oplus DES_k^{-1}(C_2) &= (M_1 \oplus k_1) \oplus (M_2 \oplus k_1) \\ &= M_1 \oplus M_2 \end{aligned}$$

由于 C_1, C_2, M_1, M_2 都是已知的，因此可以用**暴力法**，遍历 `k` 来寻找合适的 `k` 满足 $DES_k^{-1}(C_1) \oplus DES_k^{-1}(C_2) = M_1 \oplus M_2$，这需要 $C_1 2^{56}$和$C_2 2^{56}$的时间，即复杂度为$O(2^{56})$。

而解密 `k1`，只需要在找到 `k` 的基础上，通过下式解出 `k1`：

$$k_1 = M_1 \oplus DES_k^{-1}(C_1)$$

因此，总共需要2^{56} 的DES操作来破解DESW。

Problem 5

- 题目：

Problem 5 Operation mode of block ciphers. Chloé invents a new operation mode as below that can support parallel encryption. Unfortunately, this mode is not secure. Please demonstrate how an attacker knowing IV, C_0, C_1, C_2, and $M_1 = M_2 = M$ can recover M_0.

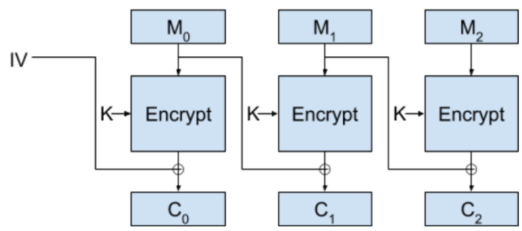

Figure 1: Chloé's invention

- 由Figure 1 可得：

$$C_0 = E(K, M_0) \oplus IV$$
$$C_1 = E(K, M_1) \oplus M_0$$
$$C_2 = E(K, M_2) \oplus M_1$$

- 而由题目已知条件可知$M_1 = M_2 = M$，所以上面三式可变形为

$$C_0 = E(K, M_0) \oplus IV$$
$$C_1 = E(K, M) \oplus M_0$$
$$C_2 = E(K, M) \oplus M$$

- 因此，可将后面的两式进行异或，得：

$$\begin{aligned} C_1 \oplus C_2 &= (E(K, M) \oplus M_0) \oplus (E(K, M) \oplus M) \\ &= E(K, M) \oplus E(K, M) \oplus M_0 \oplus M = M_0 \oplus M \end{aligned}$$

而 C_1, C_2, M 均已知，所以可以通过 $C_1 \oplus C_2 = M_0 \oplus M$ 得到 M_0.

Problem 6

- 题目：

Problem 6 **Hash functions**. One-wayness and collision-resistance are two indispensable properties of hash functions. They are in fact independent one to the other.

1. Give a function that is one-way, but not collision-resistant.
2. Give a function that is collision-resistant, but not one-way.

- 具备单向性而不具备抗冲突性的哈希函数：

$$a^x\ mod\, p,\ 如\ 2^x mod\, 5$$

  此函数不可以从输出推出输入，**满足单向性**；然而，却可以找到$x_1 \neq x_2$ 满足 $H(x_1) = H(x_2)$，如对于上面的例子，有$x_1 = 1, x_2 = 5, H(x_1) = H(x_2) = 2$，因此，**不满足抗冲突性。**

- 具备抗冲突性而不具备单向性的哈希函数：

$$H(x) = x$$

此函数不可以找到$x_1 \neq x_2$ 满足 $H(x_1) = H(x_2)$（这是单调递增函数），因此**满足抗冲突性**；然而，由于可以从输出推出输入，所以**不满足单向性。**