信息安全技术 第一次作业

18340052 何泽

Problem 1 Vigenere 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 Vigenere 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.

为确定密钥长度，分别尝试1、2、3的情况：

- 若长度为1:

$$
\begin{array}{c}
A\ B\ C\ B\ A\ B\ B\ B\ A\ C \\
A\ B\ C\ B\ A\ B\ B\ B\ A\ C
\end{array}
$$

共有2个重合

- 若长度为2:

$$
\begin{array}{c}
A\ B\ C\ B\ A\ B\ B\ B\ A\ C \\
A\ B\ C\ B\ A\ B\ B\ B\ A\ C
\end{array}
$$

共有3个重合

- 若长度为3:

$$\begin{array}{c} A\ B\ C\ B\ A\ B\ B\ B\ A\ C \\ A\ B\ C\ B\ A\ B\ B\ B\ A\ C \end{array}$$

共有1个重合

所以，密钥长度最有可能是2。

奇数序列为ACABAC，偶数序列为BBBBC，根据三个字母A, B, C的出现频率0.7, 0.2和 0.1，在奇数序列中A出现3次BC各出现1次，所以奇数序列中A就是A，而偶数序列中B出现4次C出现1次，所以B的明文是A，综上，密钥为$(0,1)=(a,b)$

Problem 3 DES

> Before 2-DES and 3-DES was invented, the researchers at RSA Labs came up with DESV and DESW, defined by
>
> $$DESV_{kk_1}(M)=DES_k(M)\oplus k1, DESW_{kk_1}(M)=DES_k(M\oplus k_1)$$
>
> In both schemes, |k| = 56 and |k1| = 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.

- DESV

对于两组不同的明文和秘文M1,C1,M2,C2，有：

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

$$C_2=DES_k(M_2)\oplus k1$$

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

那么对于满足以上条件的密钥就可以进行brute-force key search，这需要编码M_1 2^{56} 和M_2 2^{56}次，一旦找到k，就可以找到满足条件的k_1，那么总时间就是2^{56} DES。

- DESW

  此时有：

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

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

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

  那么和上面一样进行brute-force key search，需要编码C_1 2^{56} 和C_2 2^{56}次，一旦找到k，就可以找到满足条件的k_1，那么总时间就是2^{56} DES。

Problem 4 RSA

> Alice and Bob love each other, so they decide to use a single RSA modulus N for their key pairs. Of course each of them does not know the private key of the other. Mathematically, Alice and Bob have their own key pairs(e_A, d_B) and (e_B, d_B) sharing the same N. Demonstrate how Bob can derive the private key of Alice.

既然已经知道N，那么便可以将N分解为两个质数P和Q满足$P \times Q = N$，对于每一组P和Q，进而便可以通过$\phi(N) = (P-1)(Q-1)$ 计算欧拉函数，由于已经知道公钥，下面想要求私钥只需要根据公示$e_A \times d_A \ \% \ \phi(N) = 1$ 便可求得。

Problem 5 Operation mode of block ciphers

> Chloe 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, $C0, C1, C2$, and $M1 = M2 = M$ can recover $M0$.

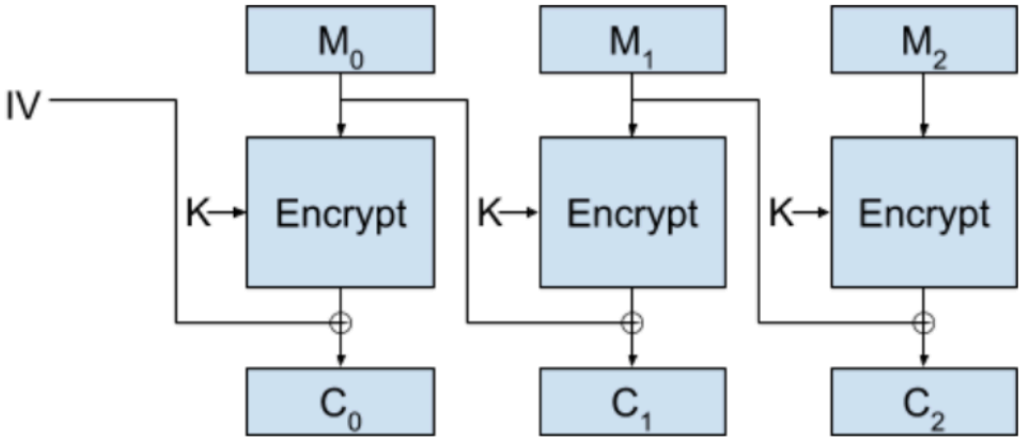

Figure 1: Chloé's invention

由于C_2是由M_1和M_2加密后的结果（M_2'）异或而得，即$C_2 = M_1 \oplus M_2'$，而$M1 = M2 = M$，即$C_2 = M \oplus M'$，由此便可以计算得到M'的值，再看C_1，$C_1 = M' \oplus M0$，而C_1也是知道的，由此便可以求出M_0的值

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.

1. 对于两个极大的数p和q，定义$h = m^e \ mod \ p \times q$

2. 令$A(x)$为任一collision-resistance函数，$B(x)$为x的最后256位，接下来另$H(x) = A(x) \ || \ B(x)$

   $H(x)$即为要寻找的函数。