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.

AB出现位置分别在1和5，相差4，有因数2，所以可能。

奇数位A出现3次，B出现1次，C出现1次，偶数位A出现0次，B出现4次，C出现1次。

$0.7 = \frac{3+4}{10}$

$0.2 = \frac{1+1}{10}$

$0.1 = \frac{1+0}{10}$

所以可能是AB。

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. $\Pr[C = c|M = m] = \frac{\Pr[C=c \wedge M=m]}{\Pr[M=m]} = \frac{\Pr[M=m|C=c]\cdot\Pr[C=c]}{\Pr[M=m]} = \frac{\Pr[M=m]\cdot\Pr[C=c]}{\Pr[M=m]} = \Pr[C = c]$
2. 设M'为猜测。

$$\begin{aligned}
&\Pr[(M' = 0 \wedge M = 0) \vee (M' = 1 \wedge M = 1)] \\
=&\Pr[M' = 0 \wedge M = 0] + \Pr[M' = 1 \wedge M = 1] \\
=&\Pr[M' = 0] \cdot \Pr[M = 0] + \Pr[M' = 1] \cdot \Pr[M = 1] \\
=&0.5 \cdot p_0 + 0.5 \cdot (1 - p_0) \\
=&0.5
\end{aligned}$$

$$
\begin{aligned}
&\Pr[M=0|C=c]\\
=&\frac{\Pr[M=0\wedge C=c]}{\Pr[C=c]}\\
=&\frac{\Pr[M=0\wedge M\oplus K=c]}{\Pr[(M=0\vee M\neq 0)\wedge C=c]}\\
=&\frac{\Pr[M=0\wedge K=c]}{\Pr[(M=0\wedge K=c)\vee(M\neq 0\wedge K\neq c)]}\\
=&\frac{\Pr[M=0]\cdot\Pr[K=c]}{\Pr[M=0]\cdot\Pr[K=c]+\Pr[M\neq 0]\cdot\Pr[K\neq c]}\\
=&\frac{p_0\cdot\Pr[K=c]}{p_0\cdot\Pr[K=c]+(1-p_0)\cdot\Pr[K\neq c]}\\
=&\begin{cases}\frac{p_0\cdot 0.4}{p_0\cdot 0.4+(1-p_0)\cdot 0.6}, & c=0\\ \frac{p_0\cdot 0.6}{p_0\cdot 0.6+(1-p_0)\cdot 0.4}, & c=1\end{cases}\\
=&\begin{cases}\frac{2\cdot p_0}{3-p_0}, & c=0\\ \frac{3\cdot p_0}{2+p_0}, & c=1\end{cases}
\end{aligned}
$$

所以$c=0$时，$p_0\geq\frac{3}{5}$则估计$M'=0$否则估计$M'=1$；$c=1$时，$p_0\geq\frac{2}{5}$则估计$M'=0$否则估计$M'=1$。

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.

DESV：对于(M,C)枚举k，计算2^{56}次$DES_k(M)$，获得中间结果m_1。枚举k_1，计算2^{64}次$C\oplus k_1$，获得中间结果m_2，比对m_1和m_2，若相等则破解k和k_1，共2^{56}次DES运算。
DESW：对于(M,C)枚举k，计算2^{56}次$DES_k^{-1}(C)$，获得中间结果m_1。枚举k_1，计算2^{64}次$M\oplus k_1$，获得中间结果m_2，比对m_1和m_2，若相等则破解k和k_1，共2^{56}次DES运算。

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.

Bob和Alice共享$p\cdot q=N$，$(p-1)(q-1)=\phi$，Bob知道Alice的公钥(e_A,N)，$\gcd(e_A,\phi)=1$且$e_A\cdot d_A \mod \phi=1$即$e_A\cdot d_A-k\cdot\phi=\gcd(e_A,\phi)$，用广义欧几里法可解$d_A$。

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.

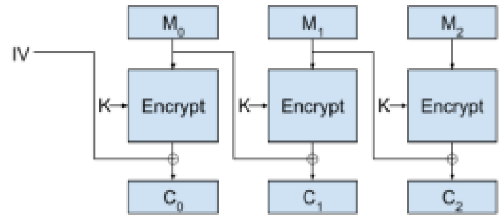

Figure 1: Chloé's invention

因为

$E(M_1, K) \oplus M_0 = C_1$

$E(M_2, K) \oplus M_1 = C_2$

所以

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

$E(M, K) \oplus M = C_2$

所以

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

所以

$M_0 = C_1 \oplus C_2 \oplus M$

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.