VE475 Intro to Cryptography Homework 1

Taoyue Xia, 518370910087

2020/05/20

1 Ex1

1. As Alice use the Caesar cipher, we can use the equation $x - \kappa \ mod \ 26$ to find the answer. After running the algorithm in python, the word "river" is the only word which can be recognized.
   So we know that Bob should meet Alice at the river, and the parameter κ is 13.

2. Let the key matrix K be a 2×2 matrix $\begin{pmatrix} a & b \\ c & d \end{pmatrix}$, then use matrix inversion to calculate K.

$$\begin{pmatrix} 3 & 14 \\ 13 & 19 \end{pmatrix} \cdot K = \begin{pmatrix} 4 & 11 \\ 13 & 8 \end{pmatrix} \ mod 26$$

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} = \begin{pmatrix} 3 & 14 \\ 13 & 19 \end{pmatrix}^{-1} \cdot \begin{pmatrix} 4 & 11 \\ 13 & 8 \end{pmatrix} \ mod 26$$

   For the plain text matrix A $\begin{pmatrix} 3 & 14 \\ 13 & 19 \end{pmatrix}$, it has $det(A) = -125$ and $gcd(-125, 26) = 1$

So $A^{-1} = \frac{1}{-125}\begin{pmatrix} 19 & -14 \\ -13 & 3 \end{pmatrix}$ And it is calculated that 21 is the inverse of -125 modulo 26, such that we get:

$$A^{-1} = \begin{pmatrix} 399 & -294 \\ -273 & 63 \end{pmatrix} = \begin{pmatrix} 9 & 18 \\ 13 & 11 \end{pmatrix} \, mod \, 26$$

Then we put A^{-1} into the initial equation:

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} = \begin{pmatrix} 9 & 18 \\ 13 & 11 \end{pmatrix} \cdot \begin{pmatrix} 4 & 11 \\ 13 & 8 \end{pmatrix} \, mod \, 26$$

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} = \begin{pmatrix} 270 & 243 \\ 195 & 231 \end{pmatrix} = \begin{pmatrix} 10 & 9 \\ 13 & 23 \end{pmatrix} \, mod \, 26$$

So we get the answer that the encryption matrix is $K = \begin{pmatrix} 10 & 9 \\ 13 & 23 \end{pmatrix}$.

3. As $n|ab$, we know that $gcd(ab, n) = n$. While $gcd(a, n) = 1$, we can deduce that $gcd(b, n) = n \ \Rightarrow \ n|b$, and the proof is done.

4.

$$\begin{aligned} 30030 \ \div \ 257 &= 116...218 \\ 257 \ \div \ 218 &= 1...39 \\ 218 \ \div \ 39 &= 5...23 \\ 39 \ \div \ 23 &= 1...16 \\ 23 \ \div \ 16 &= 1...7 \\ 16 \ \div \ 7 &= 2...2 \\ 7 \ \div \ 2 &= 3...1 \\ 2 \ \div \ 1 &= 2 \end{aligned}$$

According to the computation above, we find that $gcd(30030, 257) = 1$, which indicate that 30030 and 257 are relatively prime.

5. Set the OTP as k, and the first message as m1, the second message as m2, the first time ciphertext as c1, the second-time ciphertext as c2.

$$c1 = m1 \oplus k,\ c2 = m2 \oplus k$$
$$\Rightarrow c1 \oplus c2 = (m1 \oplus k) \oplus (m2 \oplus k) = m1 \oplus m2$$

Then attackers can use KPA to get the real key by multiple attacking, and finally get the key.

6. To be secure, it should has greater or equal to 2^{128} operations. Then the size n can be caluclated as following:

$$\begin{aligned} 2^{O(\sqrt{nlog(n)})} &\geq 2^{128} \\ nlog(n) &\geq 128^2 \\ n &\geq 1546.43 \end{aligned}$$

Then choose n to be 1547, so the size of the graph should be at least 1547.

2 Ex2

1. The Vigenère cipher is partly like the Caesar cipher, it uses a random key to decide how much it will change from plain text to ciphertext. Then it will look up in a alphabet table to finally determine the ciper-text. What's more, if the key's length is shorter than the plain text, it will be repeated.

   For example, if the plain text is "goodmorning" and the key is "beautiful", then we extend the key to be "beautifulbe", then match the ciphertext for "g" and "b", "o" and "e", etc. Finally, after looking up in the alphabet table, we will finally get the ciphertext.

2. a) As Bob send the same letter several hundred times, after being encrypted, the ciphertext will look like a paragraph fulfilled with a repeated six-letter word, because the key is six-letter long.

   b) Because Bob send the same letter a lot of times, the ciphertext is periodic with length six, so the key is six-letter long.

   c) Eve just need to add six numbers to the corresponding number of the ciphertext, and try for 26 times, then she will find the final answer.