UM-SJTU Joint Institute

Introduction to Cryptography

(Ve475)

Assignment 1

Name: Sun Yiwen ID: 517370910213
Date: May 22 2020

1 Simple questions

1. Based on the given information, we can only use the *ciphertext only* type of attack. In the case of Caesar cipher, we use the method of exhaustive search, trying all possible keys from 1-25 (0 can be skipped). For the ciphertext EVIRE, the possible plain text can be FWJSF, GXKTG, HYLUH, IZMVI, JANWJ, KBOXK, LCPYL, MDQZM, NERAN, OFSBO, PGTCP, QHUDQ, RIVER, SJWFS, TKXGT, ULYHU, VMZIV, WNAJW, XOBKX, YPCLY, ZQDMZ, ARENA, BSFOB, CTGPC, DUHQD. Among them, only RIVER and ARENA make sense, so the possible keys for this Caesar cipher are 4 and 13. RIVER and ARENA are the two possible locations for Alice and Bob's secret meeting.

2. Since $n|4$, try the value $n = 2$. Suppose K=$\begin{pmatrix} a & b \\ c & d \end{pmatrix}$, construct the equation:

$$\begin{pmatrix} 3 & 14 \\ 13 & 19 \end{pmatrix} \begin{pmatrix} a & b \\ c & d \end{pmatrix} \equiv \begin{pmatrix} 4 & 11 \\ 13 & 8 \end{pmatrix} \mod 26$$

We name $\begin{pmatrix} 3 & 14 \\ 13 & 19 \end{pmatrix}$ as matrix A. Since $\det(A) = -125$, A^{-1} exists. We can calculate:

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

$$K \equiv -\frac{1}{125} \begin{pmatrix} 19 & -14 \\ -13 & 3 \end{pmatrix} \begin{pmatrix} 4 & 11 \\ 13 & 8 \end{pmatrix} \mod 26$$

Since $(-125) \times (-5) \equiv 1 \mod 26$,

$$K = -5 \begin{pmatrix} 19 & -14 \\ -13 & 3 \end{pmatrix} \begin{pmatrix} 4 & 11 \\ 13 & 8 \end{pmatrix} = -5 \begin{pmatrix} -106 & 97 \\ -13 & -119 \end{pmatrix} = \begin{pmatrix} 530 & -485 \\ 65 & 595 \end{pmatrix} = \begin{pmatrix} 10 & 9 \\ 13 & 23 \end{pmatrix}$$

3. Since $n|ab$, there exists an integer s such that $n \times s = ab$. Since $\gcd(a, n) = 1$, there exists two integers x, y such that $ax + ny = 1$. We get $b = b(ax + ny) = abx + bny = nsx + bny = (sx + by)n$. Therefore, $n|b$.

4. Using the Euclidean algorithm,

$$30030 = 257 \times 116 + 218$$

$$257 = 218 \times 1 + 39$$

$$218 = 39 \times 5 + 23$$

$$39 = 23 \times 1 + 16$$

$$23 = 16 \times 1 + 7$$

$$16 = 7 \times 2 + 2$$

$$7 = 2 \times 3 + 1$$

$$2 = 1 \times 2$$

Therefore, $\gcd(30030, 257) = 1$. Since $16 < \sqrt{257} < 17$, if 2,3,5,7,11,13 are not factors of 257, then 257 is prime. $257 \mod 2 = 1$, $257 \mod 3 = 2$, $257 \mod 5 = 2$, $257 \mod 7 = 5$, $257 \mod 11 = 4$, $257 \mod 13 = 10$, thus we can prove that 257 is prime.

5. If the attacker can get a piece of plaintext and the corresponding ciphertext, then he can easily get the key by XORing the plaintext and the ciphertext. If the same key is used later on a new message, the attacker can easily decrypt the new message, which is why using the same key twice in OTP is dangerous.

6. To be secure, the attacker must run more than 2^{128} instructions to break the cipher. In this case, $\sqrt{n \log n} \geqslant 128$. We get $n \geqslant 4486.4$. Therefore, a graph of size 4487 should be used to be secure.

2 Vigenere cipher

1. The Vigenere cipher is a method of encrypting alphabetic text by using a series of interwoven Caesar ciphers, based on the letters of a keyword. A table of alphabets should be used in this cipher. The table has the alphabet written out 26 times in different rows, each alphabet shifted one-letter-long to the left compared to the previous alphabet. When encrypting one letter at a time, the cipher uses a different alphabet from one of the rows, where the row number depends on a repeating keyword. Decryption is performed by going to the row in the table corresponding to the key, finding the position of the ciphertext letter in that row and then using the column's label as the plaintext.

2. (a) Because if the plaintext is the same letter repeated several hundred times and the key is 6 letters long, then the ciphertext will form a loop that is 6 letters long and repeat the 6 letters over and over again. This is easy to notice and Eve will suspect it.

   (b) By counting the number of letters in the ciphertext's loop, Eve can find the key length, which is 6.

   (c) Since the plaintext is one letter repeated, Eve can try from A to Z. Using the Vigenere table, Eve can find the 26 possible keys. Suppose the plaintext Eve is currently trying is AAAAAA, then she can go to column A, find the ciphertext letters and record their corresponding row label, which will form the possible keyword. Since no English word of length six is a shift of another English word, only one of the 26 possible keys is a meaningful English word. Therefore, Eve can determine the key.