UM–SJTU Joint Institute

Electronic Circuits
(Ve311)

HW 1

Name: Ming Xingyu ID: 517370910224

1 Ex.1

1.1

Since the text is encrypted by Caesar Cypher, we can list all the possible results.
GXKTG HYLUH IZMVI JANWJ KBOXK LCPYL MDQZM NERAN OFSBO PGTCP QHUDQ *RIVER* SJWFS TKXGT ULYHU VMZIV WNAJW XOBKX YPCLY ZQDMZ *ARENA* BSFOB CTGPC DUHQD

Based on observation and my vocabulary, the text could be either RIVER or ARENA.

1.2

There are 4 letters for this word, hence, it can form a 2×2 matrix. Here for dont and ELNI, we can derive

$$\begin{pmatrix} 3 & 14 \\ 13 & 19 \end{pmatrix}$$

and

$$\begin{pmatrix} 4 & 11 \\ 13 & 8 \end{pmatrix}$$

Hence, we can have the following equation

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

$$det \begin{pmatrix} 3 & 14 \\ 13 & 19 \end{pmatrix} = -125$$

Now we need to find some x such that $-125 \cdot x \equiv 1 \ mod \ 26$. We can simply have

$$-125 = -4 \times 26 + (-21)$$

$$26 = -1 \times (-21) + 5$$

$$-21 = -4 \times 5 - 1$$

Hence, $1 = -4 \times 5 + 21 = -4 \times (26 - 21) + 21 = -4 \times 26 + 5 \times 21 = 4 \times 26 + 5 \times (-4 \times 26 + 125) = (-5) \times (-125) - 16 \times 26$, which means $-125 \times (-5) \equiv 1 \ mod \ 26$ and this matrix is invertible.

The adjacent matrix of it is

$$\begin{pmatrix} 19 & -13 \\ -14 & 3 \end{pmatrix}$$

And the inverse of it is

$$\begin{pmatrix} -95 & 70 \\ 65 & -15 \end{pmatrix}$$

Now, we can calculate the key by matrix multiplication as follows,

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} \equiv \begin{pmatrix} -95 & 70 \\ 65 & -15 \end{pmatrix} \times \begin{pmatrix} 4 & 11 \\ 13 & 8 \end{pmatrix} \bmod 26$$

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} \equiv \begin{pmatrix} 530 & -485 \\ 65 & 595 \end{pmatrix} \bmod 26$$

Finally, we have

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} = \begin{pmatrix} 10 & 9 \\ 13 & 23 \end{pmatrix}$$

1.3

Since, $n \mid ab$, we can simply derive $ab = kn,\ k \in \mathbb{N}$.
Then $b = \frac{kn}{a}$. Because $gcd(a, n) = 1 \wedge b \in \mathbb{N}$, we have $a \mid k$,
i.e. $k = ca,\ c \in \mathbb{N}$.
Hence, $b = cn \Leftrightarrow n \mid b$.

1.4

By Chinese Reminder Theorem, we can have

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

$$257 = 218 + 39$$

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

$$39 = 23 + 16$$

$$23 = 16 + 7$$

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

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

$$2 = 2 \times 1$$

Hence, $gcd(30030, 257) = 1$.

Noticing that $\sqrt[2]{257} = 16.03122$, hence, the prime factor of it can only be among 2, 3, 5, 7, 11, 13. By brutal force we can have

$$257 = 128 \times 2 + 1$$

$$257 = 85 \times 3 + 2$$

$$257 = 51 \times 5 + 2$$

$$257 = 36 \times 7 + 5$$

$$257 = 23 \times 11 + 4$$

$$257 = 19 \times 13 + 8$$

So, there is no factor for 257, which indicates 257 is prime.

1.5

We learn from the lecture that OTP use bitwise-XOR operation on the plaintext and the key.

For the XOR operation we can have $a \oplus b = c \Rightarrow a \oplus c = b$. So, for the CPCA, the enemy can derive the key and when we reuse it, the cipertext can be easily decipered.

1.6

According to the lecture slides, we know that in order to make it safe, it must let the attacker to do at least 2^128 times computation, hence,

$$\sqrt{nlogn} \geq 128$$

$$nlogn \geq 16384$$

For the algorithm implementation, the base number may varies. Here, we assume the base number to be 2. And the solution is

$$n \geq 1546.43$$

Since $n \in \mathbb{N}$, the size should be larger than 1547.

2

2.1

Firstly, for the Vigenère cipher, it has a Table, as shown below

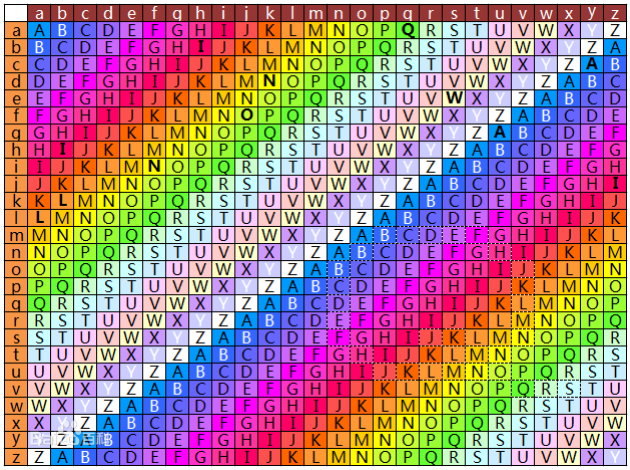

Figure 1: Vigenère cipher table.

Secondly, similar to the Caesar cipher, the principle of Vigenère cipher is to shift the letter according to the table by the key.

Then, the key is a key word, in which every letter indicate the line we look-up in the table, which will repeat itself until the length of it is the same as the plain-text during encryption.

During encryption, one letter in the key corresponding to one letter in the plain-text. For example, we have fat for the plain-text and $meat$ for the key, we have

$$f \to m \Rightarrow R$$

$$a \to e \Rightarrow E$$

$$t \to a \Rightarrow T$$

And the ciphertext is RET.

2.2

2.2.1

Since the cipher-text may repeat itself every six letters, it is reasonable for Eve to suspect the plain-text is some repeated letters with length as 1, 2, 3, 6(dividers of 6).

2.2.2

As mentioned above, the cipher-text repeated every 6 letters. The length of the key is very likely to be 6.

2.2.3

According to the helpful hint, we know that there is no English word of length 6 is a shift of another English word. If Eve guess the plain-text to be a repeated letter, she can simply look-up the dictionary to find all the English words and find which one matches the encryption.