

VE475 Homework 1

Liu Yihao 515370910207

Ex. 1 — Simple questions

1. There are totally 26 possibilities of the plain text, which are listed below:

EVIRE FWJSF GXKTG HYLHU IZMVI JANWJ KBOXK LCPYL MDQZM NERAN OFSBO
PGTCP QHUDQ RIVER SJWFS TKXGT ULYHU VMZIV WNAJW XOBKX YPCLY ZQDMZ
ARENA BSFOB CTGPC DUHQD

According to observation, RIVER and ARENA may be the secret place.

2. Since the length of the text is 4, n maybe 2, then we can construct an equation according to the plaintext *dont* and the ciphertext *ELNI*.

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

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

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

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

$$(-125) \cdot (-5) \equiv 1 \pmod{26}$$

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

$$K = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \equiv \begin{pmatrix} 9 & 18 \\ 13 & 11 \end{pmatrix} \begin{pmatrix} 4 & 11 \\ 13 & 8 \end{pmatrix} \pmod{26}$$

$$K = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \equiv \begin{pmatrix} 270 & 243 \\ 195 & 231 \end{pmatrix} \pmod{26}$$

$$K = \begin{pmatrix} 10 & 9 \\ 13 & 23 \end{pmatrix}$$

3. Suppose that $n \nmid b$, let $b = cn + d$, $n \nmid d$ and $ab = kn$, where $c, d, k \in N$, then

$$a(cn + d) = kn$$

$$ad = (k - ac)n = \frac{ad}{n}n$$

We know $k - ac$ is an integer, so $\frac{ad}{n}$ is also an integer. However, since $\gcd(a, n) = 1 \Rightarrow n \nmid a$ and $n \nmid d$, it makes a contradiction, so $n \mid b$.

4.

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

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

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

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

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

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

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

$$2 = 2 \times 1$$

$$\gcd(30030, 257) = 1$$

Since $16 < \sqrt{257} < 17$, so the factors of 257 can only be 2, 3, 5, 7, 11, 13, we can try them one by one. $257 \bmod 2 = 1$, $257 \bmod 3 = 2$, $257 \bmod 5 = 2$, $257 \bmod 7 = 5$, $257 \bmod 11 = 4$, $257 \bmod 13 = 10$. Then we can concluded that 257 is prime.

5. If the attacker got the pair of a plaintext and its corresponding ciphertext of length l , he can just XOR the plaintext and the ciphertext to get the key of length l . When another message ciphered with the same key was sent, the attacker can easily decipher the ciphertext and steal the message. So using the same key twice in the OTP is dangerous.
6. Since secure means that the attacker has to compute at least 2^{128} operations to break the encryption,

$$\sqrt{n \log n} \geq 128$$

$$n \geq 4486.43$$

So a graph with a size of 4487 should be used to be secure.

Ex. 2 — Vigenère cipher

- 1.
2. a)
b)
c)

Ex. 3 — Programming

Uploaded to Canvas.