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 HYLUH 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*.

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

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

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

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

$$(-125) \cdot (-5) \equiv 1 \bmod 26$$

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

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

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

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

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 $\dfrac{ad}{n}$ 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.

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

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

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 mod 2 = 1, 257 mod 3 = 2, 257 mod 5 = 2, 257 mod 7 = 5, 257 mod 11 = 4, 257 mod 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 twive in the OTP is dangerous.

6. Since secure means that the attacker has to compute at least 2^{128} operations to break the encrypton,

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

$$n \geqslant 4486.43$$

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

Ex. 2 — Vigenère cipher

1. Suppose we have a plaintext of length l and a key of length n. First, if $n < l$, we repeat it for several times until it reach a length of l. Then, for each letter in the plaintext, we shift it by the value of the key letter of the same index as the letter, using the method similar to Caesar cipher.

   For convenience, we obtain a Vigenère square, or Vigenère table, shown in Figure 1. We can find the encrypted letter at the cross of the plaintext letter and the corresponding key letter.

   When we want to decrypt the ciphertext, we can choose the row of the corresponding key letter and find the position of the letter in the ciphertext, then the letter of that column is the plaintext letter in that place.

2. a) If the plaintext is a same letter repeating hundreds of times, and the key have a length of l, then the ciphertext will have a loop every l letters, it will be very obvious to observe in this circumstance. So Eve can suspect it.

   b) Eve can count the letters in each loop and easily find $l = 6$.

   c) Eve can choose each of 26 letters one by one and compare with the first six letters of the ciphertext. According to the Vigenère square, he can get 26 possible keys with six letters. Since no English word of length six is a shift of another English word, only one of the 26 keys is the correct key, Eve can determine it with the help of an English dictionary.

	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
A	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
B	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A
C	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B
D	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C
E	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D
F	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E
G	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F
H	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G
I	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H
J	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I
K	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J
L	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K
M	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L
N	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M
O	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N
P	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O
Q	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P
R	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q
S	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R
T	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S
U	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T
V	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U
W	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V
X	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W
Y	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X
Z	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y

Figure 1: Vigenère square

Ex. 3 — Programming

Uploaded to Canvas.