VE475 Homework 1

Yiwen Yang 519370910053

Ex.1 - Simple Questions

1. Use brute force to list all possible plain text with the key κ from 0 to 25, the results are shown as:

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

   Then through observation, the most possible plain text is RIVER, so Bob should go to the river to meet Alice.

2. (a) Text *dont* consists of 4 characters, so block size n should satisfy that $n \mid 4$. Try $n = 2$.

   (b) The order of *dont* in alphabet is $[3, 14, 13, 9]$, and ELNI is $[4, 11, 13, 8]$. Construct the equation as

   $$A = \begin{pmatrix} 3 & 14 \\ 13 & 9 \end{pmatrix}$$
   $$\begin{pmatrix} 3 & 14 \\ 13 & 9 \end{pmatrix} \cdot \begin{pmatrix} a & b \\ c & d \end{pmatrix} \equiv \begin{pmatrix} 4 & 11 \\ 13 & 8 \end{pmatrix} \bmod 26$$

   (c) Since $det(A) = -125$, $gcd(-125, 26) = 1$, then A is invertible modulo 26. Calculate the inverse of -125 modulo 26

   $$\begin{aligned} -125 &= -5 \times 26 + 5 \\ 26 &= 5 \times 5 + 1 \\ 1 &= 26 - 5 \times 5 \\ &= (-5) \times (-125) + (-24) \times 26 \\ (-125)^{-1} &= (-5) \end{aligned}$$

   The inverse of A is

   $$\begin{aligned} A^{-1} &= -\frac{1}{125} \begin{pmatrix} 19 & -14 \\ -13 & 3 \end{pmatrix} \\ &= \begin{pmatrix} -95 & 70 \\ 65 & -15 \end{pmatrix} \\ &\equiv \begin{pmatrix} 9 & 18 \\ 13 & 11 \end{pmatrix} \bmod 26 \end{aligned}$$

Calculate the key as

$$\begin{aligned} K = \begin{pmatrix} a & b \\ c & d \end{pmatrix} &= A^{-1} \cdot \begin{pmatrix} 4 & 11 \\ 13 & 8 \end{pmatrix} \\ &= \begin{pmatrix} 9 & 18 \\ 13 & 11 \end{pmatrix} \cdot \begin{pmatrix} 4 & 11 \\ 13 & 8 \end{pmatrix} \\ &= \begin{pmatrix} 270 & 243 \\ 195 & 231 \end{pmatrix} \\ &\equiv \begin{pmatrix} 10 & 9 \\ 13 & 23 \end{pmatrix} \bmod 26 \end{aligned}$$

So the encryption matrix is $\begin{pmatrix} 10 & 9 \\ 13 & 23 \end{pmatrix}$.

3. Since $n \mid ab$, then $\exists m \in \mathbb{Z}^*$ such that $ab = mn$.

   From $gcd(a, n) = 1$, one can find $x, y \in \mathbb{Z}^*$ such that $ax + ny = 1$.

   Then

$$\begin{aligned} b &= b(ax + ny) \\ &= abx + bny \\ &= mnx + bny \\ &= n(mx + by) \end{aligned}$$

   Since m, x, b, y are all integers, then $n \mid b$.

4. (a)

$$\begin{aligned} 30030 &= 116 \times 257 + 218 \\ 257 &= 1 \times 218 + 39 \\ 218 &= 5 \times 39 + 23 \\ 39 &= 1 \times 23 + 16 \\ 23 &= 1 \times 16 + 7 \\ 16 &= 2 \times 7 + 2 \\ 7 &= 3 \times 2 + 1 \\ 2 &= 2 \times 1 + 0 \end{aligned}$$

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

   (b) Since $\lfloor \sqrt{257} \rfloor = 16$, check prime numbers less than 16 which are $[2, 3, 5, 7, 11, 13]$ and non of the numbers is a divisor of 257, prooving that 257 is prime.

5. Since the key of One Time Pad is very easy to calculate given plain text and cipher text, so it is very likely for Eve to observe a second time usage of the key in a known plaintext attack, which is not safe.

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

$$\sqrt{n \log n} \geq 128$$
$$n \geq 4487$$

Hence the size of the graph should be at least 4487.

Ex.2 - Vigenère Cipher

1. Vigenère cipher is designed based on Caesar shift cipher. In Caesar cipher, every plain text character is mapped to the cipher text character by adding a Caesar shift n, where $0 \leq n \leq 25$. To encrypt a Vigenère cipher, first define a key K with length l. For each character in plain text with index i, find the corresponding shift key in K as $k_i = K_{i \bmod l}$ (K_p is the pth character of K). Then, construct a Caesar shift n_i on the plain text character, where n_i is the shifting number of plain text A to Caesar cipher k_i. Apply to all of the characters in plain text, one will get a Vigenère cipher. To decrypt the cipher, simply find all corresponding Caesar unshift with K.

   Vigenère cipher utilizes multiple Caesar ciphers in a loop of the key length to achieve the encryption, and the reference table is shown in Table 1.

   For example, to encrypt plain text TORADORA with key TAIGA, find corresponding Caesar shift for the key as

$$T \rightarrow \text{Caesar shift } 19$$
$$A \rightarrow \text{Caesar shift } 0$$
$$I \rightarrow \text{Caesar shift } 8$$
$$G \rightarrow \text{Caesar shift } 6$$
$$A \rightarrow \text{Caesar shift } 0$$

   Then repeating the 5 Caesar shift on the plain text TORADORA yields

$$T \rightarrow \text{Caesar shift } 19 \rightarrow M$$
$$O \rightarrow \text{Caesar shift } 0 \rightarrow O$$
$$R \rightarrow \text{Caesar shift } 8 \rightarrow Z$$
$$A \rightarrow \text{Caesar shift } 6 \rightarrow G$$
$$D \rightarrow \text{Caesar shift } 0 \rightarrow D$$
$$O \rightarrow \text{Caesar shift } 19 \rightarrow H$$
$$R \rightarrow \text{Caesar shift } 0 \rightarrow R$$
$$A \rightarrow \text{Caesar shift } 8 \rightarrow I$$

Then the Vigenère cipher for this example is MOZGDHRI. It can be observed that same characters in the plain text such as A, have very different ciphers as G and I. This makes the word frequency attack on Caesar cipher become extremely difficult.

	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
0	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
1	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
2	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
3	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
4	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
5	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
6	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
7	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
8	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
9	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
10	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
11	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
12	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
13	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
14	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
15	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
16	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
17	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
18	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
19	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
20	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
21	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
22	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
23	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
24	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
25	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

Table 1: Vigenère Cipher

2. (a) When Eve has the copy of the cipher text, he will find that the cipher repeats itself at a certain length (in this example 6), indicating that the Bob is sending the same letter.

   (b) Observe the cipher and find the least cycle period, then the period is the key length.

   (c) Extract any 6 letters from the cipher text, apply Caesar unshift n ($n = 0, 1, \ldots, 25$) on the cipher text to get 26 possible shifted keys. Since no English word with 6 letters is a shift of another one, observe all these 26 keys and their shifted version to find an English word, then the word will be the key.

Ex.3 - Programming

See in folder **ex3**.