VE475 Homework 1

Anna Li
Student ID: 518370910048

Problem 1

1.

We try every situations for the ciphertext "EVIRE", and get the 25 situations by switching K from 0 to 25, and find that there are two possibilities: river when K = 13 and arena when K = 4

2.

First, we could convert dont and ELNI into 2×2, which is:

$$dont = \begin{pmatrix} 3 & 14 \\ 13 & 19 \end{pmatrix} \quad ELNI = \begin{pmatrix} 4 & 11 \\ 13 & 8 \end{pmatrix} \tag{1}$$

suppose the encryption matrix is K, we can get:

$$K = dont^{-1} \cdot ELNI \mod 26 \tag{2}$$

$$dont^{-1} = \frac{1}{125} \begin{pmatrix} -19 & 14 \\ 13 & -3 \end{pmatrix} \mod 26 = \begin{pmatrix} -95 & 70 \\ 65 & -15 \end{pmatrix} \tag{3}$$

$$K = \begin{pmatrix} 10 & 9 \\ 13 & 23 \end{pmatrix} \tag{4}$$

3.

since $n|ab$, we could deduce that

$$\exists r \in \mathbb{R}, nr = ab$$

since $gcd(a, n) = 1$, we could deduce that

$$\exists s, t \in \mathbb{R}, as + nt = 1$$

Therefore

$$b = b(as + nt) = nrs + bnt = n(rs + bt)$$

Therefore, $n|b$

4.

$$\begin{aligned} 30030 &= 257 \times 116 + 218 \\ 257 &= 218 \times 1 + 39 \\ 218 &= 39 \times 5 + 23 \\ 39 &= 23 \times 1 + 16 \\ 23 &= 16 \times 1 + 7 \\ 16 &= 7 \times 1 + 9 \\ 7 &= 9 \times 0 + 7 \\ 9 &= 7 \times 1 + 2 \\ 7 &= 2 \times 3 + 1 \\ 2 &= 1 \times 2 + 0 \end{aligned} \tag{5}$$

Therefore, gcd(30030,257)=1
since $\sqrt{257} \in (16, 17)$, we could check 2,3,5,7,11,13
since

$$gcd(257, 2) = 1 \quad gcd(257, 3) = 1 \quad gcd(257, 5) = 1$$

$$gcd(257, 7) = 1 \quad gcd(257, 11) = 1 \quad gcd(257, 13) = 1$$

Therefore, 257 is a prime number

5.

if the attacker get the ciphertext and part of the plaintext, they will solve out the key soon. Therefore, when the next time the one time pad use the same key, the attacker could easily solve the whole plaintext. Therefore, this is dangerous.

6.

Since secure means that the attacker has to compute at least 2^128 operations to break the encryption it suffices to calculate.

$$\sqrt{n \log n} = 128 \Rightarrow n = 4487$$

Therefore, at least 4487 size of graph should be used

Problem 2

1.

Vigenere Cipher is a method of encryption, which is similar to ceaser cipher but is more secure than it. In the Vigenere cipher, we first choose a keyword with n length, and then repeat it. This keyword means that how many steps should the letter shift in each position.
And we could look up this table to encrypt the plain text:

	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

Fig. 1: Table of Vigenere cipher

2.

a)

Because the cipher text repeats the same six letters several hundred times, and the relative position difference between the cipher text is the same as the difference between the key. Therefore, Eve can suspect that the plain text is one repeated letter.

b)

Since the cipher text always repeat with period of 6, Eve can guess the key length

c)

Eve could shift this repeated six letters from 0 to 25, and find out the only one possibility, since no English word of length six is a shift of another English word.