VE475 Introduction to Cryptography
Homework 1

Jiang, Sifan
jasperrice@sjtu.edu.cn
515370910040

May 19, 2019

Ex. 1 - Simple questions

1. Since Alice uses Caesar cipher and we already known the ciphertext, we can apply CCA to decrypt the ciphertext, "EVIRE". So, the 25 possible names of the place are: *duhqd*, *ctgpc*, *bsfob*, *arena*, *zqdmz*, *ypcly*, *xobkx*, *wnajw*, *vmziv*, *ulyhu*, *tkxgt*, *sjwfs*, *river*, *qhudq*, *pgtcp*, *ofsbo*, *neran*, *mdqzm*, *lcpyl*, *kboxk*, *janwj*, *izmvi*, *hyluh*, *gxktg*, or *fwjsf*. However, only "*arena*" and "*river*" are meaningful, which could be the meeting place.

2. Since the length of plaintext *dont* is 4, reasonable size of the key should be 2×2. Label letters as integers from 0 to 25, the plaintext then is $\begin{pmatrix}3 & 14 & 13 & 19\end{pmatrix}$ and the ciphertext is $\begin{pmatrix}4 & 11 & 13 & 8\end{pmatrix}$. After splitting the letters, we would have

$$\underbrace{\begin{pmatrix}3 & 14\\ 13 & 19\end{pmatrix}}_{A} \cdot \begin{pmatrix}a & b\\ c & d\end{pmatrix} \equiv \begin{pmatrix}4 & 11\\ 13 & 8\end{pmatrix} \mod 26$$

   Since $\det(A) = -125$ and $\gcd(-125, 26) = 1$, A is invertible modulo 26. Also, we can obtain that -5 is the multiplicative inverse of -125 modulo 26 by applying extended Euclidean algorithm. We can then calculate

$$\begin{aligned}
K = \begin{pmatrix}a & b\\ c & d\end{pmatrix} &\equiv \begin{pmatrix}3 & 14\\ 13 & 19\end{pmatrix}^{-1} \cdot \begin{pmatrix}4 & 11\\ 13 & 8\end{pmatrix} \mod 26\\
&\equiv \frac{1}{-125} \cdot \begin{pmatrix}19 & -14\\ -13 & 3\end{pmatrix} \cdot \begin{pmatrix}4 & 11\\ 13 & 8\end{pmatrix} \mod 26\\
&\equiv \frac{1}{-125} \cdot \begin{pmatrix}-106 & 97\\ -13 & -119\end{pmatrix} \mod 26\\
&\equiv \begin{pmatrix}530 & -485\\ 65 & 595\end{pmatrix} \mod 26\\
&\equiv \begin{pmatrix}10 & 9\\ 13 & 23\end{pmatrix} \mod 26
\end{aligned}$$

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

3. We can suppose that $n|b$ is wrong, which gives $b = kn + d$, where k and d are integers and $d \in (0, n)$. Since $n|ab$, we would have $ab = ln$, where l is an integer. After combining

two relations above, we have

$$\begin{aligned} a(kn+d) &= ln \\ akn + ad &= ln \\ ad &= (l-ak)n \\ \frac{ad}{n} &= l - ak \end{aligned}$$

Since $l - ak$ is an integer, so should $\frac{ad}{n}$ be an integer. However, since $\gcd(a, n) = 1$ and $d \in (0, n)$, which gives $n \nmid a$ and $n \nmid d$, $\frac{ad}{n}$ could not be an integer. So, the assumption is wrong and $n|b$.

4. Applying Euclidean algorithm

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

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

Since $16^2 = 256 < 257 < 289 = 17^2$, the factor of 257 could only be obtained from 2, 3, 5, 7, 11, and 13. However, none of these primes can exact divide 257. So, 257 is a prime.

5. Once Eve got the key and if the same key is used to encrypt the plaintext, Eve can easily break the ciphertext by using the key to XOR the ciphertext, which can be seen from tab 1.

Table 1: Truth table.

a	k	$a \hat{} k$	$(a \hat{} k) \hat{} k$
1	1	0	1
1	0	1	1
0	1	1	0
0	0	0	0

6. Being secure meaning it should take at least 2^{128} operations to break the encryption. So

$$\begin{aligned} \sqrt{n \log n} &\geq 128 \\ n &\geq 4486.4 \end{aligned}$$

So, the size of 4487 (or larger) should be used for the graph to be secure.

Ex. 2 - Vigenère cipher

1. The main idea of Vigenère cipher is to use Caesar ciphers on each single letter but with different shifts (keys). To clearly explain how Vigenère cipher works, an example would be used.

If we are going to encrypt “goodmorning”, basically, we need to first have a key word we same length of the plaintext. Here, we use “havenicetea”. Now for each letter in the plaintext, we can find the letter at the top row. Then, find the corresponding key letter at the left column. With two letters, we can find a letter in the table, which is illustrated in fig 1.

Conducting the procedure above for each letter in the plaintext, and finally we would get the ciphertext, “NOJHZWTRBRG”.

	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: Standard Vigenère cipher table.

2. a) Since the ciphertext has a repeating pattern, Eve can make sure that the plaintext must be something repeated. And based on some guess, Eve can suspect that the plaintext is one repeated letter.

   b) By looking for the repeating pattern of the ciphertext and counting the number of letters in each loop, Eve can easily obtain the length $l = 6$.

   c) Eve can choose one letter from 26 letters as the plaintext that Bob sent. And with the ciphertext, she can get 26 different possible keys with 6 letters. Since no English word of length six is a shift of another English word, she can try to shift though possible keys to find the real key.

Ex. 3 - Programming