UM-SJTU JOINT INSTITUTE
VE475 Introduction to Cryptography

Homework 1

Li Yong 517370910222

May 21, 2021

Ex.1 Simple questions

1. If the key is 4, the plaintext is "ARENA".
   If the key is 13, the plaintext is "RIVER".

2. Let the key K be
$$K = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$$
   Then
$$\underbrace{\begin{pmatrix} 3 & 14 \\ 13 & 19 \end{pmatrix}}_{A} \cdot \begin{pmatrix} a & b \\ c & d \end{pmatrix} \equiv \begin{pmatrix} 4 & 11 \\ 13 & 8 \end{pmatrix} \bmod 26$$
$$K = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \equiv \begin{pmatrix} 3 & 14 \\ 13 & 19 \end{pmatrix}^{-1} \cdot \begin{pmatrix} 4 & 11 \\ 13 & 8 \end{pmatrix} \bmod 26$$
$$det(A) = -125 \Rightarrow det(A) \cdot (-5) \equiv 1 \bmod 26$$
   So that A is invertible modulo 26 and
$$A^{-1} = -\frac{1}{125} \begin{pmatrix} 19 & -14 \\ -13 & 3 \end{pmatrix} \bmod 26$$
   -5 is the inverse of -125 modulo 26, such that
$$A^{-1} = \begin{pmatrix} -95 & 70 \\ 65 & -15 \end{pmatrix} \equiv \begin{pmatrix} 9 & 18 \\ 13 & 11 \end{pmatrix} \bmod 26$$
$$K = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \equiv \begin{pmatrix} 9 & 18 \\ 13 & 11 \end{pmatrix} \cdot \begin{pmatrix} 4 & 11 \\ 13 & 8 \end{pmatrix} \bmod 26$$
$$K = \begin{pmatrix} 10 & 9 \\ 13 & 23 \end{pmatrix}$$

3. If $n \mid ab$, then
$$ab = cn, c \in \mathbb{Z}.$$
   And $\gcd(a, n) = 1$, then there exists two integers s and t, such that
$$as + nt = 1$$
   Multiplying by b, we get
$$asb + ntb = b$$
$$b = ncs + ntb$$
$$b = n(cs + tb)$$
   Hence $n|b$.

4.

$$\begin{aligned} 30030 &\equiv 218 \bmod 257 \\ 257 &\equiv 39 \bmod 218 \\ 218 &\equiv 23 \bmod 39 \\ 39 &\equiv 16 \bmod 23 \\ 23 &\equiv 7 \bmod 16 \\ 16 &\equiv 2 \bmod 7 \\ 7 &\equiv 1 \bmod 2 \\ 2 &\equiv 1 \bmod 1 \end{aligned}$$

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

$$30030 = 2 \times 3 \times 5 \times 7 \times 11 \times 13$$

These primes are all less than $\sqrt{257}$, hence 257 is prime.

5. Key, plaintext and ciphertext are in the same length. The message with the same key is definitely in the same length. If an attacker knows the key, it will reminds the attacker to use the known key to decrypt the ciphertext. Hence it is dangerous to use the same key twice in the OTP.

6.

$$\begin{aligned} \sqrt{n \log n} &\geq 128 \\ n &\geq 4487 \end{aligned}$$

Ex.2 Vigenère cipher

1. The Vigenère cipher encrypts with a table 1 (Vigenère square or Vigenère table) which consists of 26 Caesar ciphers in sequence with different shift values. To encrypt, we choose a keyword and repeats it until its length equals to the plaintext's so that we get the key. As for the first letter in the plaintext, we use the Caesar cipher corresponding to the first letter in the key. Then for the second letter of the plaintext, we use the second letter in the key and so on.

	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 or Vigenère table

2. a) Both the plaintext and the key are repeated so that the ciphertext is repeated, the cycle of which is the least common multiple of lengths of the plaintext and the keyword. And the cycle is of 6 letters. Regards to repeating so much times, it probably is one repeated letter.

   b) $\text{lcd}(1, 6) = 6$, so that Eve can guess the key length is 6.

   c) The ciphertext can also be regarded that the keyword was encrypted by one-letter-key in the Vigenère cipher. Hence, Eve can just decrypt it as a simple Caeser cipher.

Ex.3 Programming

Uploaded with this PDF.