37

Introduction to Cryptography: Homework #1

Due on May 24, 2019 at 3:10pm

Professor Manuel

ShiHan Chan

Problem 1

Part One

Since ciphertext 'EVIRE' is the only available information, enumerate all possible key K is only solution to find the plaintext (Ciphertext only attack). Enumerate all possible Caesar cipher key K from 0 to 25:
The plaintext is a meaningful word only when K=4,13,: Bob needs to meet Alice at 'ARENA' or 'RIVER'.

Part Two

Firstly, transfer both the plaintext "dont" and ciphertet "ELNI" to numerical value (alphabet a z corresponding to 0 25).
"dont" is trasfered to "3 14 13 19", and "ELMI" is trasfered to "4 11 13 8".
Since $n|4$, guess n=2 (guess the key is a 2x2 matrix K) with gcd(det(K),2)=1. K=

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} \tag{1}$$

And we can get

$$\begin{pmatrix} 3 & 14 \\ 13 & 19 \end{pmatrix} \begin{pmatrix} a & b \\ c & d \end{pmatrix} \equiv \begin{pmatrix} 4 & 11 \\ 13 & 8 \end{pmatrix} \mod 26 \tag{2}$$

Since det(A)= det($\begin{pmatrix} 3 & 14 \\ 13 & 19 \end{pmatrix}$) = -125 $\neq$ 0, A^{-1} exists

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

$$K \equiv \frac{-1}{125} \begin{pmatrix} 19 & -14 \\ -13 & 3 \end{pmatrix} \begin{pmatrix} 4 & 11 \\ 13 & 8 \end{pmatrix} \mod 26 \tag{4}$$

Since (-125)*(-5) $\equiv$ 1 mod 26 After calculation,

$$K \equiv 625 * \frac{-1}{125} \begin{pmatrix} 19 & -14 \\ -13 & 3 \end{pmatrix} \begin{pmatrix} 4 & 11 \\ 13 & 8 \end{pmatrix} \mod 26 \tag{5}$$

$$K \equiv \begin{pmatrix} -95 & 70 \\ 65 & -15 \end{pmatrix} \begin{pmatrix} 4 & 11 \\ 13 & 8 \end{pmatrix} \mod 26 \tag{6}$$

$$K \equiv \begin{pmatrix} 530 & -485 \\ 65 & 595 \end{pmatrix} \mod 26 \tag{7}$$

$$K \equiv \begin{pmatrix} 10 & 9 \\ 13 & 23 \end{pmatrix} \mod 26 \tag{8}$$

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

Part Three

Assume r is an integer such that nr=ab. Since gcd(a,n)=1, there exists two integers x,y that satiesfy ax+ny=1.
Then b=b(ax+ny)=abx+bny=nrx+nby=n(rx+by)
so n | b

Part Four

Applying the extended euclidean algorithm, 30300 = 257 * 117 +231
257 = 231 * 1 + 26
231= 26 * 8 + 23
26 = 23 * 1 + 3

Problem 1 continued on next page...

$23 = 3 * 7 + 2$
$3 = 2 * 1 + 1$
$2 = 1 * 2$
So gcd(30300,257)=1 (30300 and 257 are coprime)
Since $16 < \sqrt{257} < 17$, checking 2,3,5,7,11, 13 are not factors of 257 can prove 257 is prime. 257 mod 2=1,257 mod 3=2,257 mod 5=2,257 mod 7=5,257 mod 11=4, 257 mod 13 = 10. So 257 is prime.

Part Five

If the attacker get a piece of corresponding plaintext and ciphertext of length L, he can get the key of length L by XOR on plaintext and ciphertext. The attacker can easily decipher the ciphertext if the plaintext is sent by the same key next time. That explains why same using same key twice in the OTP is dangerous.

Part Six

Secure means that the attacker has to compute at least 2^{128} operations to break the encryption. So $\sqrt{nlogn}$ must greater than 128 to secure.
$\sqrt{nlogn} >= 128$ implies $n >= 4486.4$ So a graph with size 4487 should be used to secure.

Problem 2

Vigenere cipher is a substitution cipher. Given plaintext and the key, if the length of plaintext is longer thanf the key, repeat the key until the length of the key and plaintext are same.
There is a 26 x 26 table like the graph below. And each neighboring pair of row/column shift one space compared to each other.

	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

When plaintext encrypts into ciphertext, each character of plaintext should be found on left column, and each corresponding charactor of key should be found on upper row, and the character in the table which are on the same line of both plaintext and key is the ciphertext.
For example, if the plaintext is ATT and the key is LE. Repeat the key LE and get keystream LEL. Through looking up the table, A and L corresponds to L, T and E corresponds to X, T and L corresponds to E, so the ciphertext is LXE.
When ciphertext decrypts into plaintex, we find the column of corresponding key charactor and position of letter in the ciphertext, then the letter of the corresponding row is the plaintext.
(a)If the plaintext is the same letter repeated several hundred of time, and the key is L letters long English word, the ciphertext will have a loop every L letters, it's very obvious and Eve can suspect it. (ciphertext will have a loop every lcm(length of unrepeated plaintext in plaintext, length of key) letters if plaintext repeats)
(b) Eve can count the letters in each loop in ciphertext and find L = 6.
(c) There are 26 possible plaintext choices since plaintext is one repeated letter. Eve can guess each choices one by one and compare plaintext to the first six ciphertext to get the key. So there are 26 possible keys in total. Since there is no English word of length six is a shift of nother English word, only one of 26 possible key is the correct key.

Problem 3

Programming part

makefile has some issues
-3