Quiz. 1

(Deadline March 07, 2024)

Department: 資工系 **Student ID: 109550198** **Name:** 卜銳凱

Problem 1

Given the ciphertext:

C UYGHARMZ IUWMPRWIR GAIR YVRMP

MBHMZWMPUM C VMMXWPE YV PYR VCZ

ZMGYQMD VZYG CXCZG YP CPCXKTWPE CPD MBHXYZM

RNM VXYYD YV CDQCPUMD OPYSXMDEM SNWUN MCUN

KMCZ LZWPEI SWRN WR

a) Please write a program to find out the frequencies of letters in the ciphertext.

"109550198.py"

b) Use the plaintext frequency count information below as a reference to break these encrypted messages.

A COMPUTER SCIENTIST MUST OFTEN

EXPERIENCE A FEELING OF NOT FAR

REMOVED FROM ALARM ON ANALYZING AND EXPLORE

THE FLOOD OF ADVANCED KNOWLEDGE WHICH EACH

YEAR BRINGS WITH IT

c) Assume C is ciphertext, and P is plaintext. Can you find a particular relationship between C and P?

Ans) The comparison table is in the bottom table.

Table 1: Ciphertext letter frequency count: (times)

A	B	C	D	E	F	G	H	I	J	K	L	M
2	2	12	6	4	0	5	3	4	0	2	1	19
N	O	P	Q	R	S	T	U	V	W	X	Y	Z
5	1	12	2	9	3	1	6	7	9	6	12	9

Table 2: Common frequency of letters appearance: (%)

E	A	R	I	O	T	N	S	L	C	U	D	P
11.16	8.5	7.58	7.54	7.16	6.95	6.65	5.74	5.49	4.54	3.63	3.38	3.17
M	H	G	B	F	Y	W	K	V	X	Z	J	Q
3.01	3.0	2.47	2.07	1.81	1.78	1.29	1.10	1.01	0.29	0.27	0.20	0.20

Table 3: Ciphertext to plaintext mapping

Ciphertext	A	B	C	D	E	F	G	H	I	J	K	L	M
	0	1	2	3	4	5	6	7	8	9	10	11	12
Plaintext	U	X	A	D	G	J	M	P	S	Q	Y	B	E
	20	23	0	3	6	9	12	15	18	16	24	1	4
Ciphertext	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
	13	14	15	16	17	18	19	20	21	22	23	24	25
Plaintext	H	K	N	V	T	W	Z	C	F	I	L	O	R
	7	10	13	21	19	22	25	2	5	8	11	14	17

d) Suppose "$f(x) = ax + b \bmod 26$", where x is plaintext, please solve the value of a and b.

f(0)=b(mod26)=2
f(1)=a+b(mod26)=11

after calculation, we get a = 9, b = 2

e) What is the key size of the Mono-Alphabetic Substitution Cipher? Such a size makes exhaustive search becomes difficult?

Ans) 26! which does make exhaustive search becomes difficult.

f) (Bonus) Please try to see if it is possible to decipher this problem with ChatGPT or another tool.

Ans) It is challenging to decrypt a problem using tools like ChatGPT, explores key space size in affine cipher encryption, and requires finding inverses in a given set.

Problem 2

Plaintext is encrypted using an affine cipher. A plaintext symbol, x, is drawn from Z_{30} and, hence, encryption is defined as "$y = ax + b \bmod 30$", where y *is* the resulting ciphertext and the encryption key is given by $k_{enc} = (a, b)$.

a) Determine the size of the key space (that is, the total number of keys).

- The number of possible values for a is 8 (values coprime with 30).
- The number of possible values for b is 30 (any value in Z_{30}).
- Therefore, the size of the key space is 8×30=240.

b) Determine all values in Z_{30} that have inverses and, by trail-and-error, determine the inverses.

The values in Z_{30} that have inverses and their respective inverses are:

1 with inverse 1
7 with inverse 13
11 with inverse 11
13 with inverse 7
17 with inverse 23
19 with inverse 19
23 with inverse 17
29 with inverse 29

These inverses are calculated based on the property that an element $a \in Z_{30}$ has a multiplicative inverse if gcd(a,30)=1, using the Extended Euclidean Algorithm to find such inverses.

c) An attacker intercepts the following plaintext/ciphertext pairs:

x	y
4	8
10	26
27	7

Determine the encryption key $k_{enc} = (a, b)$.

$8 = 4a + b \bmod 30$
$26 = 10a + b \bmod 30$
$7 = 27a + b \bmod 30$

After analyzing the given plaintext/ciphertext pairs and iterating over possible values of a, the encryption key was found to be:
a=13
b=16

d) Determine the decryption key $k_{dec} = (c, d)$, where "$x = cy + d \bmod 30$".

Using the modular inverse of the encryption key a and adjusting for b, the decryption key was determined as:
c=7, which is the modular inverse of a=13
d=8, calculated to reverse the encryption process