Quiz. 1

(Deadline March 07, 2024)

Problem 1

Given the ciphertext:

C UYGHARMZ IUWMPRWIR GAIR YVRMP
A COMPUTERSCIENTIST MUST OFTEN

MBHMZWMPUM C VMMXWPE YV PYR VCZ
EXPERIENCE A FEELING OF NOT FAR

ZMGYQMD VZYG CXCZG YP CPCXKTWPE CPD MBHXYZM
REMOVED FROM ALARMUN ANALYZING AND EXPLORE

RNM VXYYD YV CDQCPUMD OPYSXMDEM SNWUN MCUN
THE FLOOD OF ADVANCED KNOWLEDGE WHICH EACH

KMCZ LZWPEI SWRN WR
YEAR BRINGS WITH IT

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

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

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

J

Q

a=9

b=2

20×a+2 = 26×i

23×a+2 = 26×k+1

26 52 78 104

220 1×a+2

130 180 156

f(x) = ax+b

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

Follow the table 3. #

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

$a = 9 + 26i$ (i is any integer)

$b = 2 + 26k$ (k is any integer) #

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

26! #

∵ 26! 相對於 2^{88}，所以需要花費許多時間 #

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

Problem 2

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

30 : 1, 2, 3, 5, 6, 10, 15, 30

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

$8 \times 30 = 240$ #

b) Determine all values in $\mathbb{Z}_{30}$ that have inverses and, by trail-and-error, determine the inverses.

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

x	y
4	8
10	26
27	7

$8 = 4a + b \bmod 30$

$26 = 10a + b \bmod 30$

$7 = 27a + b \bmod 30$

30 | 367

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

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

b) 1, 7, 11, 13, 17, 19, 23, 29 #

$1 \times 1 \equiv 1 \pmod{30}$

$7 \times 13 \equiv 1 \pmod{30}$

$11 \times 11 \equiv 1 \pmod{30}$

$13 \times 7 \equiv 1 \pmod{30}$

$23 \times 17 \equiv 1 \pmod{30}$

$17 \times 23 \equiv 1 \pmod{30}$

$19 \times 19 \equiv 1 \pmod{30}$

$29 \times 29 \equiv 1 \pmod{30}$ #

(c)

$k_{\text{enc}} = (a, b) = (13, 16)$ #

$4 \times 13 + 16$

$4 \times 19 + 22$

$4 \times 17 + 0$

$4 \times 23 + 6$

$4 \times 29 + 12$

(d)

$k_{\text{dec}} = (c, d) = (7, 16)$ #

$d(x) = a^{-1}(x - b) \bmod m$

11

$c = 7$

$7(8 - b) \bmod 30 = 4$

22

$7(7 - b) \bmod 30 = 27$

70

34 64 94

124

154

Problem 1

(f)

I will now fill out the mapping table with these initial guesses and more based on the frequency match-up. Let's proceed with this assumption and adjust as necessary. Based on frequency analysis and initial guesses, here is the potential mapping from ciphertext to plaintext:

- M→E
- C→A
- Y→R
- P→O
- R→I
- Z→N
- W→S
- V→T
- U→L
- X→C

- W→S
- V→T
- U→L
- X→C
- D→U
- G→D
- N→M
- I→H
- E→F
- H→G
- S→B
- A→Y
- B→W
- Q→P
- K→K
- T→V

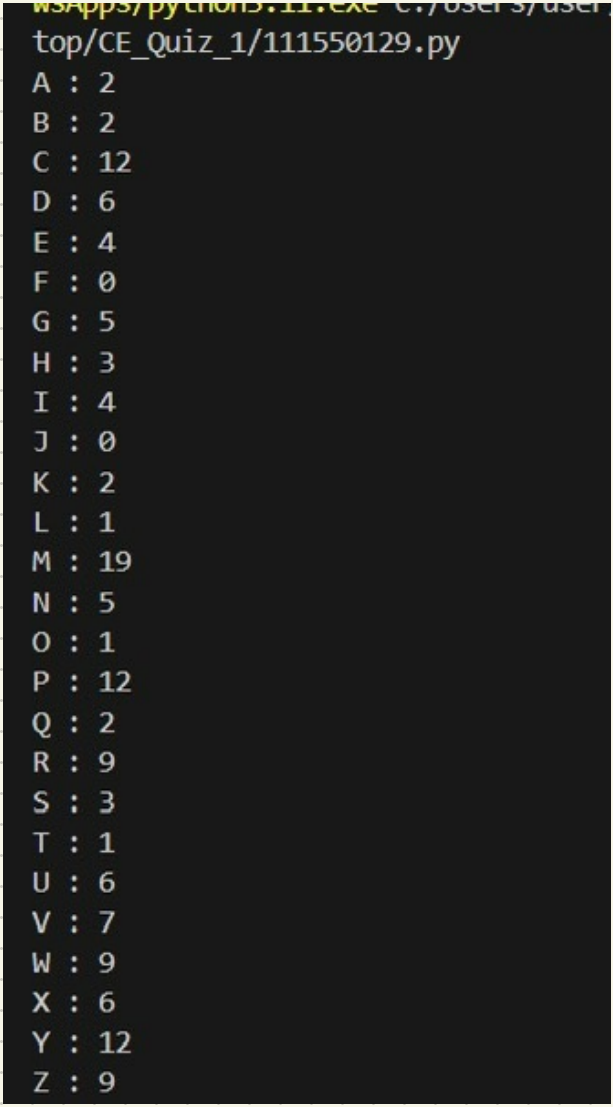
- A→Y
- B→W
- Q→P
- K→K
- T→V
- O→J
- L→Q

```
T : 1
U : 6
V : 7
W : 9
X : 6
Y : 12
Z : 9
```

Here is the result of the Chatgpt.

The answer is incorrect.

程式結果截圖


top/CE_Quiz_1/111550129.py
A : 2
B : 2
C : 12
D : 6
E : 4
F : 0
G : 5
H : 3
I : 4
J : 0
K : 2
L : 1
M : 19
N : 5
O : 1
P : 12
Q : 2
R : 9
S : 3
T : 1
U : 6
V : 7
W : 9
X : 6
Y : 12
Z : 9