Quiz. 1

(Deadline March 07, 2024)

Problem 1

Given the ciphertext:

A computer scientist
U AKENCZGT WASGHZSWZ ECWZ KJZGH

GLNGTSGHAG U JGGBSHM KJ HKZ JUT

TGEKFGD JTKE UBUTE KH UHUBORSHM UHD GLNBKTG

knowledge
ZPG JBKKD KJ UDFUHAGD YHKIBGDKG HPSAP

GUAP OGUT XTHSMW ISTP SZ
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
6	6	2	6	5	2	19	13	2	7	13	2	3
N	O	P	Q	R	S	T	U	V	W	X	Y	Z
3	2	5	0	1	9	10	12	0	4	1	1	8

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	C	L	V	D	m	V	e	h	w	t	o	X	g
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	p	r	h	q	z	i	r	A	j	s	B	k	t

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

$3x + 20 \pmod{26}$

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

e) What is the key size of the Mono-Alphabetic Substitution Cipher? Such a size makes exhaustive search becomes difficult? $26!$

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 $k_{\text{enc}} = (a, b)$.

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

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

$4a + b = 8$

$10a + b = 26$

$21a + b = 7$

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

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

Quiz. 1

(Deadline March 07, 2024)

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.

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	5	3	4	2	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													
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													

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

```
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
```

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

Table 1: Ciphertext letter frequency count: (times)

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?

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	V	X	A	D	G	J	M	P	S	V	Y	B	E
	21	23	0	3	6	9	12	15	18	21	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	Q	T	W	Z	C	F	I	L	O	R
	7	10	13	16	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.

猜C為A 猜MR是IT $a=9$ $b=2$

$0 \cdot a+b = 2$ $19 \cdot a+b = 19$

$8 \cdot a+b = 22$

e) What is the key size of the Mono-Alphabetic Substitution Cipher? Such a size makes exhaustive search becomes difficult? 26!, Yes, it is about 2^{88}, too big to search

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

quipquip.com 可直接解密

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

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

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

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 $k_{\text{enc}} = (a, b)$.

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

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

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

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

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													
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													

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

a 與 n 要互質才能有inverse

a 可能值

與30互質 {1, 7, 11, 13, 17, 19, 23, 29} => 8個

b 有30個

key space is 8×30 = 240

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

此題是求 Z_{30} 內有相互逆元的數

計算可得知

(1, 1) (17, 23)

(7, 13) (19, 19)

(23, 17)

(11, 11)

(29, 29)

(13, 7)

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

x	y
4	8
10	26
27	7

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

(C)

$4a+b \equiv 8 \pmod{30}$

$10a+b \equiv 26$ ……

$27a+b \equiv 7$ ……

$6a \equiv 18$ 位数为 8, 1

$17a \equiv 11$

故 a = ~~3~~, 13

$a = 13$

$b = 16$

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

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

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													
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				A									
				0	.								

$29 \times 9 + 8$

$(13, 7)$

$16 \times 7 + d \equiv 0 \pmod{30}$

$C = 11$

$112 + d \equiv 0$

$98 + 8$

$d \equiv 8$

$147 + 8$

147

A: $c = 7$

$d = 8$