

# Quiz1

Department:資工

Student ID:110550085

Name:房天越

1. Please write a program to find out the frequencies of letters in the ciphertext down below.
2. Use these plaintext frequency count information as a reference to break this encrypted messages.

Ans: 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

3. Assume C is Ciphertext, P is Plaintext. Can you find out a particular relationship in between C and P?

Ans: Shown in the chart below.

4. Suppose  $f(x) = ax + b \pmod{26}$  where x is plaintext, please solve the value of a and b.

Ans:  $a=3, b=19$

5. What is the key size of the mono alphabetic substitution cipher? Such size make exhaustive search becomes difficult?

Ans: 26!

6. (Bonus) What is the key space in this affine substitution cipher we solved

$f(x) = ax + b$  ?

Ans:  $12 \times 26 = 312$ , because a need to be coprime with 26, and b can be from 0 to 25.

Ciphertext:

T ZJDMBYFS VZRFGYRVY DBVY JIYFG  
FKMFSRFGZF T IFFARGL JI GJY  
ITS SFDJEFC ISJD TATSD JG  
TGTANQRGL TGC FKMAJSF  
YOF IAJJC JI TCETGZFC XGJHAFCLF HORZO  
FTZO NFTS WSRGLV HRYO RY

Ciphertext's letter frequency count:

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
6	2	6	5	2	19	12	0	7	12	2	4	3	2	5	0	1	9	9	12	0	4	1	1	9	6

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

Cipher	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	L	U	D	M	V	E	N	W	F	O	X	G	P
	11	20	3	12	21	4	13	22	5	14	23	6	15

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
Y	H	Q	Z	I	R	A	J	S	B	K	T	C
24	7	16	25	8	17	0	9	18	1	10	19	2