Quiz1

Department:資工系　　Student ID:110550164　　Name:游建峰

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.

The plaintext:

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?

對照表在最底下那張表格裡面。

4. Suppose f(x) = ax + b (mod 26) where x is plaintext, please solve the value of a and b.

a=3 + 26 * i, where i is any integer

b=19 + 26 * j, where j is any integer

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

The key size of the mono alphabetic substitution cipher: 26!

因為 26!大概有 2^88 那麼大，所以用暴力解會花一段時間

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

f(x)= ax+b ?

因為在小於 26 的數字中，有 12 個數字和 26 互質，再加上 b 有 26 個可能的值(0~25)所以可能的鑰匙總共有 12 * 26 = 312。

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