Quiz1

Department: **Student ID:** **Name:**

1. Please write a program to find out the frequencies of letters in the ciphertext down below.

=> Feel free to ask TA if you have question

2. Use these plaintext frequency count information as a reference to break this 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

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

=> A->T, B->W, C->Z, D->C, E->F, F->I, G->L, H->O, I->R, J->U, K->X, L->A, M->D, N->G, O->J, P->M, Q->P, R->S, S->V, T->Y, U->B, V->E, W->H, X->K, Y->N, Z->Q

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

=> f(0) = b (mod 26) = 19

f(1) = a + b (mod 26) = 22

after calculation, we get a = 3, b = 19

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

=> 26!

6. (Bonus) What is the key space in this affine substitution cipher we solved f(x)= ax+b ?

=> In the affine substitution cipher f(x) = 3x + 19, the multiplication key is 3 and the additive key is 19. To calculate the size of the key space, we need to determine the number of possible values for the multiplication key and the additive key that are valid within the affine cipher.

For the multiplicative key, we need to choose a value that is relatively prime to 26,

So the possible choices for multiplicative key are :

1, 3, 5, 7, 9, 11, 15, 17, 19, 21, 23, 25 , total 12 choices.

For the additive key, we can choose any integer between 0 and 25,

So the possible choices for additive key are : 0, 1, 2, …, 25 , total 26 choices.

Thus, the size of key space is the number of possible combinations : 12 x 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

Encryption

Plaintext	A	B	C	D	E	F	G	H	I	J	K	L	M
x	0	1	2	3	4	5	6	7	8	9	10	11	12
Ciphertext	T	W	Z	C	F	I	L	O	R	U	X	A	D
f(x)	19	22	25	2	5	8	11	14	17	20	23	0	3

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
G	J	M	P	S	V	Y	B	E	H	K	N	Q
6	9	12	15	18	21	24	1	4	7	10	13	16