Q6) As in my folder, there is kripto.py. folder which give me the number of coincidence when we shift the tex. According to so where most common coincidences appear when shift by 7, 14, 21. From the result, i estimate that keylength is 7 when i grouped them by 7 i.

I divide the text into subgroups in my code line 13. When i apply the frequency analysis for ~~those~~ groups i've

1.

$\overset{14}{O}$ $\overset{18}{S}$ $\overset{24}{Y}$

k_1 = K !

e i

2

$\overset{15}{P}$ $\overset{13}{D}$ $\overset{18}{S}$

k_2: L

E S H

3

$\overset{4}{E}$ $\overset{19}{T}$ $\overset{0}{A}$

k_3 = a

4

$\overset{4}{E}$ $\overset{14}{O}$

k_4: W

I S

5

$\overset{12}{M}$ $\overset{0}{A}$ $\overset{22}{W}$

k_5: 8

4 18 14

6

$\overset{22}{W}$ $\overset{6}{G}$

k_6: S

e O

7

$\overset{13}{N}$ $\overset{3}{D}$ $\overset{25}{Z}$

k_7 A 14 4 0

Q1) ciphertext = N Z W O   k=?

N:13   plaintext = 13-k (mod 26)

Z:25

W:22

O:14

	N	Z	W	O
k= 1 →	M	Y	V	N
2 →	L	X	U	M
3 →	K	W	T	L
4 →	J	V	S	K
5 →	I	U	R	J
6 →	H	T	Q	I
7 →	G	S	P	H
8 →	F	R	O	G
9 →	E	Q	N	F
10 →	D	P	M	E
11 →	C	O	L	D

$\boxed{k = 8,\ 11}$

Q2) We know A → H

$0 \quad 7$

(α, β)

$$0 \cdot \alpha + \beta \equiv 7$$

↓

7

H C

↓ ↓

~~A~~ ? → in English C can be: "N", "m", "S", "T"

"N" → C

$13 \cdot \alpha + 7 \equiv 2$

$13 \cdot \alpha \equiv 21 \pmod{26}$

↓

we can not find any α value since 13 divides 26. remainer can be 0 or 13. SO plainletter canot be N.

"m" → C "S" → C

$14 \cdot \alpha \equiv 21 \pmod{26}$ | $18 \cdot \alpha \equiv 21 \pmod{26}$

They can not since 14 and 18 are even number, and 26 is even, remainer should be even either.

"T" → C

$19 \cdot \alpha \equiv 21 \pmod{26}$

LAST OPTION

If choose α as 23. the encryption supports.

We found $\alpha = 23$ and $\beta = 7$. for decryption key:

$23^{-1} \equiv 17 \pmod{26}$ $\alpha_d = 17$ $\gamma = 11.$

0 : A → H : 7
1 : B → E : 4
2 : C → B : 1
3 : D → Y : 24
4 : E → V : 21
5 : F → S : 18
6 : G → –
7 : H → M : 12
8 : I → J : 19
9 : J → –
10 : K → D : 3
11 : L → A : 0
12 : M → X : 23

13 : N → U : 20
14 : m → X : 23
15 : O → R : 17
16 : P → –
17 : Q → –
18 : R → I : 8
19 : S → F : 5
20 : T → C : 12
21 : U → Z : 25
22 : V → –
23 : W → T : 19
24 : Y → N : 13
25 : Z → –
~~25~~ :

A successful man Is one who can lay a firm foundation with the bricks others have thrown at him.

Q3) Since our alpabet is bigram and 31 letters in it the modulo should be 31* 31 = 961. This is our modulo. And for the beta value gcd(a,b)! = 1.

Beta can be any value between 0 - 960. Because it just shifts. However, alpha can not take any value that has gcd(a,b) != 1. Since 31 is prime, only the factors of 31 can not be alpha. Since 961 is 31.31

$\# \alpha = 961 - 31 = \underline{\underline{930}}$.

Total key space is 961 * 930 = 893730

Q5) k = {S, A, N, I, T, Y,} = k = {18, 0, 13, 8, 19, 24}

A RRNNQW TB IGQOEE BAYL Q·HMLRAOA WG

0 17 17 13 13 16 22 19 1 8 6 16 14 4 4 1 0 24 11 16 7 12 11 17 0 14 0 22 6

-18 -0 -13 -8 -19 -24 -18 -0 -13 -8 -19 -24 -18 -0 -13 -8 -19 -24 -18 -0 -13 -8 -19 -24 -18 -0 -13 -8 -19

8 / 17 4 5 20 18 4 / 19 14 / 0 13 18 22 4 17 / 19 7 0 19 / 16 20 4 18 19 8 14 13 14 13

I REFUSE TO ANSWER THAT QUESTION ON.

R2E T2HSFDF BAYL I QWG'R CNBE MFW

17 25 4 19 25 7 18 5 3 5 1 0 24 11 8 16 22 6 17 2 13 1 4 12 5 22

-24 -18 -0 -13 -8 -19 -24 -18 -0 -13 -8 -19 -24 -18 -0 -13 -8 -19 -24 -18 -0 -13 -8 -19 -24 -18

19 7 4 6 17 14 20 13 3 18 19 7 0 19 8 3 14 13 19 10 13 14 22 19 7 4

THE GROUNDS THAT I DONT KNOW THE

AAAPCJ

0 0 0 15 2 9

-0 -13 -8 -19 -24 -18

0 13 18 22 4 17

ANSWER.