Q1 P.T Syed Mohammad Irteza

(1.1)

K=3

0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25
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

0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25
D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C

C.T= VBHG PRKDPPDG LUWHCD

(1.2)

Z HORYHSDNLVWDQ

WE LOVE PAKISTAN

Q3 Vigenere Cipher.

P.T= KTWO IS THE HIGHEST PEAK OF PAKISTAN

10	19	22	14	8	18	19	7	4	7	8	6	7	4	18	19	15	4	0	10	14	5	15	0	10	8	18	19	0	13
K	T	W	O	I	S	T	H	E	H	I	G	H	E	S	T	P	E	A	K	O	F	P	A	K	I	S	T	A	N

key = FASTNUCES.

F	A	S	T	N	U	C	E	S
5	0	18	19	13	20	2	4	18

K	T	W	O	I	S	T	H	E	H	I	G	H	E	S	T	P	E	A	K	O	F	P	A	K	I	S	T	A
F	A	S	T	N	U	C	E	S	F	A	S	T	N	U	C	E	S	F	A	S	T	N	U	C	E	S	F	A
5	0	18	19	13	20	2	4	18	5	0	18	19	13	20	2	4	18	5	0	18	19	13	20	2	4	18	5	0

C.T= PTOHVMVLWMIYARMVTWFKGYCUMMKYAF

Q2 Monoalphabetic Ciphers:—

C.T. = BNCEPQCBEAQBEBIMPFNIYQAEAEYCPMHVMAY
CMQP

Frequency:—

E	5	Y	3
Q	4	N	2
B	4	I	2
C	4	F	1
A	4	H	1
M	4	V	1
P	3		

Frequency Table:—

E	12.7	R	6.0	G	2.0	Q	0.10
T	9.1	O	4.3	Y	2.0	Z	0.07
A	8.2	I	4.0	P	1.9		
O	7.5	C	2.8	B	1.5		
I	7.0	U	2.8	V	1.0		
N	6.7	M	2.4	K	0.8		
S	6.3	W	2.4	J	0.15		
H	6.1	F	2.2	X	0.15		

First we will MAP all the characters according to the most frequent letters with common english letters.

	Positions		Positions
E → E	4,9,13,24,26	Y → H	21,27,35
Q → T	6,11,17,22,38	N → R	2,19
B → A	1,8,12,14	I → D	15,20
C → O	3,7,28,36	F → I	18
A → I	10,23,25,34	H → C	31
M → N	16,30,33,37	V → U	22
P → S	5,29,39		

AFTER Substitution, we get,

AROETTAOREATEDINDRTHERETEIOSHNCUNIH
SONTS

AROES·TOAEITAEADNTIRDHTIEIEHOSNCUNIH
ONTS

C.T = AROESTOAEITAEADNTIRDHTIEIEHOSNCUNIH
ONTS

After Substitution there are some readalle words are appearing, Now by using digrams and some more refinments, we can change into to readable String :—

AROES can be AROSE
To will be To
A will be A (AEITA can be A+ET or IT)
Now moving forwards.

AEITAEA let assume A + ET , suggesting

A can be a part of a word AREA or A TIME

Let Take it as :-

AROSE TO A TIME

Now Remaining DONT looks like DONT can be assume :- and IRDHTIEIEHO

IR can IS , IN , ARE , R
AFTER analysis This String can be

HITHER DIRT , HIDE , THIRD , HIT
RETHEIR , REHIT

By Substituting, Our STRING Form readable form more and more.

AROSE TO A TIME DONT REHIT

Now lets define the rest of the String.

OSNC | UNIHONTS

let take OSNC, If we analyze SNC Sounds like SINCE, It can be used, It can be SONC sounds like SONS

Next UNIHONTS, If we analyze

UNIHONT: can be Sounds like UNITE or can be UNITES

So, our final decryption will be

AROSE TO A TIME DONT REHIT SINCE UNITE

Q4

4.1 PT=ATTACK POSTPONED UNTIL TWOAM

KEY = IRTEZA ∴ According to Lexicography key will be :

IRTEZA
1 2 3 4 5 6
6 4 1 2 3 5

1	2	3	4	5	6
a	t	t	a	c	K
P	O	S	T	P	O
N	E	D	U	n	t
I	L	t	W	O	A
M	V	W	X	y	Z

we can use dummy alphabets to fill, as can use spaces.

when we use white spaces to fill the remainings the PT, we get maybe not as the original. It is called irregular case

Now arranging CT according to our lexicographic order key.

C.T = KOTAZATUWXAPNIMTOELVTSDTWCPNOY

C.T = KOTA_ATUW_APNIMTOEL_TSDT_CPNO_

Decryption

1	2	3	4	5	6
A	T	T	A	C	K
P	O	S	T	P	O
N	E	D	U	N	T
I	L	T	W	O	A
M	V	W	X	Y	Z

Now read Row wise

ATTACKPOSTPONEDUNTILTWOAM

Rest VWXYZ was the dummy alphabets.

Now with spaces, let see what we get :—

1	2	3	4	5	6
A	T	T	A	C	K
P	O	S	T	P	O
N	E	D	U	N	T
I	L	T	W	O	A
M	_	_	_	_	_

P-T is Same.

4.2 P-T = SAVEYOURSELFWEAREDISCOVERED

key = PAKISTAN

Since key has repetative character which is a unique case, we will remove the second repetative letter from the key.

key = PAKISTN

Now PAKISTN ≈ AIKNPST

1234567 2437156

1	2	3	4	5	6	7
s	a	v	e	y	o	u
r	s	e	l	f	w	e
a	r	e	d	i	s	c
o	v	e	r	e	d	z

ASRVELDR VEEE UECZ SRAO YFIE OWSD

DECRYPTION

1	2	3	4	5	6	7
s	a	v	e	y	o	u
r	s	e	l	f	w	e
a	r	e	d	i	s	c
o	v	e	r	e	d	z

Save yourself we are discovered.

Q#5

Encryption

```
T       L       R       O       I       O       E       N       E
  H   -   A   O   E   F   R   -   S   L   C   T   D   I   -   H
    E       H       -       T       -       A       -       T
      R       R       A       O       A       E       O       W
-   O T   E   N   P   R   -   F   L   H   R   ,   -   L   -   A
  N       H       -       T       -       O       S       D
    E       I
  L   D   C   T   .
L       -       Y
```

C.T= TLROIOENERRAOAEOWEIH_AOEFR_SLCTDI_H_OTENPR_
FLHR,_L_ALDCT.EH_T_A_TNH_T_OSDL_Y

Total = 76 (dot + spaces)

Decryption

T				L				R				O				I				O				E				N				E
	H		-		A		O		E		F		R		-		S		L		C		T		D		I		-		H	
		E				H				-				T				-				A				-				T		
			R				R				A				O				A				E				O				W	
-		O		F		E		N		P		R		-		F		L		H		R		'		-		L		-		A
	N				H				-				T				-				O				S				D			
		E				I																										
	L		O		C		T		.																							
L				-				Y																								

P.T = THE_LAHORE_FORT_IS_LOCATED_IN_THE_NORTHERN_PART_OF_LAHORE'S_OLD_WALLED_CITY.

Q.6 C.T. = WWLHVAUZNODYEILAEQIOMNA

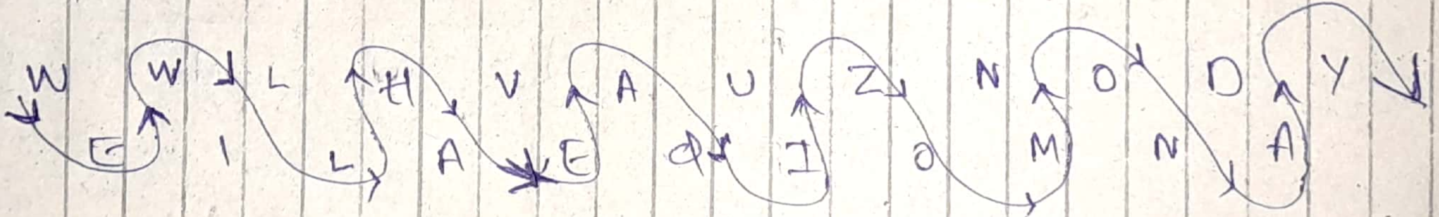
TOTAL charaters = 23

Divide key 2 as dept = 2

$\frac{23}{2} \approx 11.5 \approx 12$ ∴ Divide the string After 12th character

C.T. = WWLHVAUZNODY | EILAEQIOMNA

Now write is Rail form



P.T WEWILLHAVEAQUIZONMONDAY