





## Q<sup>3</sup> Monoalphabetic Cipher -

C.T. = BNCEPQCBEAQBEBIMPFNIYQAEAEYCPMHVMAY  
CMQF

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	0.6
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	→ C	Y	→ H
Q	→ T	N	→ R
B	→ A	I	→ D
C	→ O	F	→ I
A	→ I	H	→ C
M	→ N	V	→ U
P	→ S		

AFTER Substitution, we get,

ARQETTAORREATEDINDRTHRETEIOSHNCUNITH  
SONTS



(2)

AR OES TO AE IT AE AD NT IR D HT IE IE HO S NC UN IH  
O N T S

C.F. = AR OES TO AE IT AE AD NT IR D HT IE IE HO S NC UN IH  
O N T S

After Substitution these are some readable words are appearing, Now by using digrams and some more refinements, we can change into to readable strings -

AR OES can be AROSE

To will be To

A will be A (AE ITA can be A+ET or IT)

Now moving forwards -

AE IT AE let assume A ~~AE~~ + ET, suggesting

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

Let Take it as :-

AROSE TO A TIME

Now Remaining DNT looks like DONT  
can be assume :- and IR D HT IE IE HO

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

HITHER ~~DIRT~~ 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 text of the String.

OSNC UNITHONTS

let take OSNC, if we analyze SNC sounds like SINCE, it can be used, it can be SONC sounds like SONS

Next UNITHONTS, if we analyze

UNITHONT: 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 2 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.

Now arranging CT according to our Lexicographic order key.

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

C.T = KOTAZATUWXAPNIMTOELVTSOTWCPNOY

C.T<sub>2</sub> KOTA\_ATUW-APNIMTOEL-TSOT-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

ATTACK POSTPONED UNTIL TWOAM

Rest VWXYZ was the dummy alphabets.

Now with spaces, let see what we get:-



Q. 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 repetitive characters which is a unique case, we will remove the second repetitive letter from the key.

Key = PAKISTN

Now PAKISTN  
 1 2 3 4 5 6 7 ≈ AIKNPST  
 2 4 3 7 1 5 6

P A K I S T N  
 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 VEEFUECZ SRAO  
 YFIEDWSD

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

CT = TLROIDENERRAOAEOWEIH-AOEFR-SLETDI-H-OTENPR-  
FLHR'-L-ALDET.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	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	R	-	F	L	H	R	'	-	L	-	A
N	H	-	T	-	O	S	O								
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. = WWLHVAVUZ NODYEILAEQIOMNA

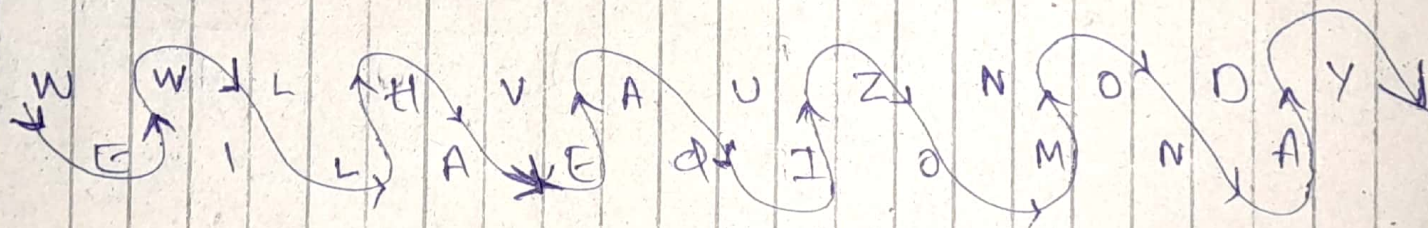
TOTAL characters = 23

Divide by 2 as dept = 2

$\frac{23}{2} \approx 11.5 \approx 12 \therefore$  Divide the string after 12<sup>th</sup> character

C.T. = WWLHVAVUZ NODYEILAEQIOMNA

Now write in Rail form



P.T WE WILL HAVE A QUIZ ON MONDAY