CMR INSTITUTE OF TECHNOLOGY
(UGC AUTONOMOUS)
Approved by AICTE | Accredited by NAAC with 'A' Grade
All B. Tech Programs Accredited by NBA

STUDENT REPORT

DETAILS

Name

A MANAS KUMAR

Roll Number

20R01A67C1

EXPERIMENT

Title

WEEK 1

Description

Implementation of cryptanalysis on caesar cipher

Procedure and Overvation:

Input:

Here
is a sample Encrypted Message:

GFS
WMY OG LGDVS MF SFNKYHOSU ESLLMRS, PC WS BFGW POL DMFRQMRS, PL OG CPFU M UPCCSKSFO HDMPFOSXO GC OIS LMES DMFRQMRS DGFR SFGQRI OG CPDD GFS LISSO GK LG, MFU OISF WS NGQFO OIS GNNQKKSFNSL GC SMNI DSOOSK. WS NMDD OIS EGLO CKSJQSFODY GNNQKKPFR DSOOSK OIS 'CPKLO', OIS FSXO EGLO GNNQKKPFR DSOOSK OIS 'LSNGFU' OIS CGDDGWPFR EGLO GNNQKKPFR DSOOSK OIS

'OIPKU', MFU LG GF, QFOPD WS MNNGQFO CGK MDD OIS UPCCSKSFO DSOOSKL PF OIS HDMPFOSXO LMEHDS. OISF WS DGGB MO OIS NPHISK OSXO WS WMFO OG LGDVS MFU WS MDLG NDMLLPCY POL LYEAGDL. WS CPFU OIS EGLO GNNQKKPFR LYEAGD MFU NIMFRS PO OG OIS CGKE GC OIS 'CPKLO' DSOOSK GC OIS HDMPFOSXO LMEHDS, OIS FSXO EGLO NGEEGF LYEAGD PL NIMFRSU OG OIS CGKE GC OIS 'LSNGFU' DSOOSK, MFU OIS CGDDGWPFR EGLO NGEEGF LYEAGD PL NIMFRSU OG OIS CGKE GC OIS 'OIPKU' DSOOSK, MFU LG GF, QFOPD WS MNNGQFO CGK MDD LYEAGDL GC OIS NKYHOGRKME WS WMFO OG LGDVS.

Step:1

OPen
the encrypted message only in Notepad.

Step2:

Find
the frequency of each letter in the encrypted message. to
find the frequency of all the letters appearing in the intercept. For
this intercept we get the values given in the table below.

Ciphertext Letter	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
Frequency	5	2	26	42	23	51	67	8	33	1	35	39	35	29	85	30	14	17	88	0	17	3	16	6	10	0

Ciphertext Letter	S	O	G	F	D	L	K	M	I	P	N	C	E	R	U	W	Q	Y	H	X	A	V	B	J	T	Z
Frequency	88	85	67	51	42	39	35	35	33	30	29	26	23	17	17	16	14	10	8	6	5	3	2	1	0	0

Step3:

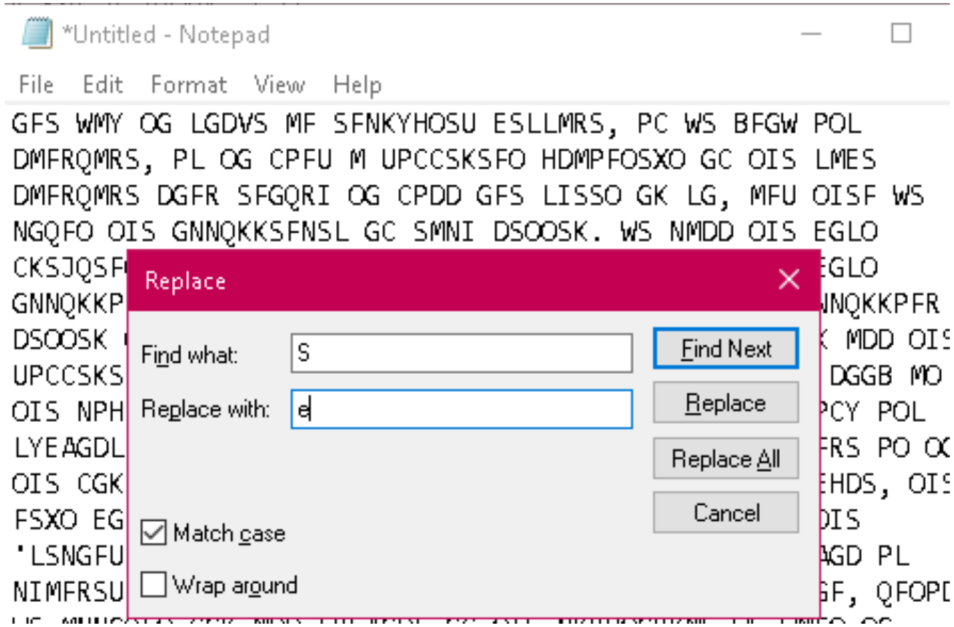
Follow
the table below to find the characters to be substituted for the
given encrypted message.

Table 1 Frequency of characters in English

Letter	*Frequency*	*Letter*	*Frequency*	*Letter*	*Frequency*	*Letter*	*Frequency*
E	12.7	H	6.1	W	2.3	K	0.08
T	9.1	R	6.0	F	2.2	J	0.02
A	8.2	D	4.3	G	2.0	Q	0.01
O	7.5	L	4.0	Y	2.0	X	0.01
I	7.0	C	2.8	P	1.9	Z	0.01
N	6.7	U	2.8	B	1.5		
S	6.3	M	2.4	V	1.0		

Step4:

Click
ctrl+H in the notepad



Click
the check box: Match case

Step
5:

Start
substituting one by one letters by following the sequence

S
→ e
O
→ t
I
→ h
G
→ o
F
→ n
M
→ a
X
→ x

W
→ w
B
→ k
U
→ d
D
→ l
K
→ r
P
→ i
L
→ s
V
→ v

H
→ p
A
→ b
X
→ x
Y
→ y
E
→ m
N
→c
C→f
R
→g
Q
→ u
J
→ q

Step 6:

Final decrypted text will be as shown below.

Output :

```
one way to solve an encrypted message, if we know its language, is to find a different plaintext of the sa
me language long enough to fill one sheet or so, and then we count the occurrences of each letter. we call
the most frequently occurring letter the 'first', the next most occurring letter the 'second' the followin
g most occurring letter the 'third', and so on, until we account for all the different letters in the plai
ntext sample. then we look at the cipher text we want to solve and we also classify its symbols. we find t
he most occurring symbol and change it to the form of the 'first' letter of the plaintext sample, the next
most common symbol is changed to the form of the 'second' letter, and the following most common symbol is
changed to the form of the 'third' letter, and so on, until we account for all symbols of the cryptogram w
e want to solve.
```

V

Q) ----------is the science and art of transforming messages to make them secure and immune to attack.

Cryptography

Q) The _____ is the original message before transformation

Plaintext

Q) A Caesar cipher is an example of a

Substitution cipher

Q) The field of both cryptography and cryptanalysis is

Cryptology

Q) The ------ is the message after transformation

Ciphertext