Mahavir Education Trust's

SHAH & ANCHOR KUTCHHI ENGINEERING COLLEGE

Chembur, Mumbai - 400 088

UG Program in Information Technology

Experiment No: 01				
Date of Performance:	15/07/2024			
Date of Submission:	12/08/2024			
Program Formation/ Execution/ Correction (06)	**Timely Submission (01)**	**Viva (03)**	**Experiment Marks (10)**	**Teacher Signature with date**

EXPERIMENT - 01

AIM : Monoalphabetic Substitution Cipher using Frequency Analysis Method

❖ BREAKING THE SHIFT CIPHER :

1. **Brute-Force Attack**:

- Try all 26 possible shifts.
- Check for readable output with each shift.

2. **Frequency Analysis**:

- Compare letter frequencies in the ciphertext to common letters (e.g., 'E', 'T') in English to estimate the shift.

3. **Known Plaintext**:

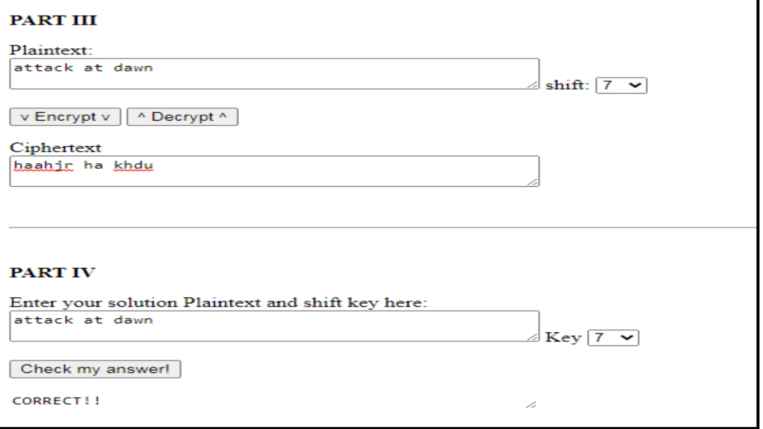
- If you know part of the plaintext, use it to calculate the shift.

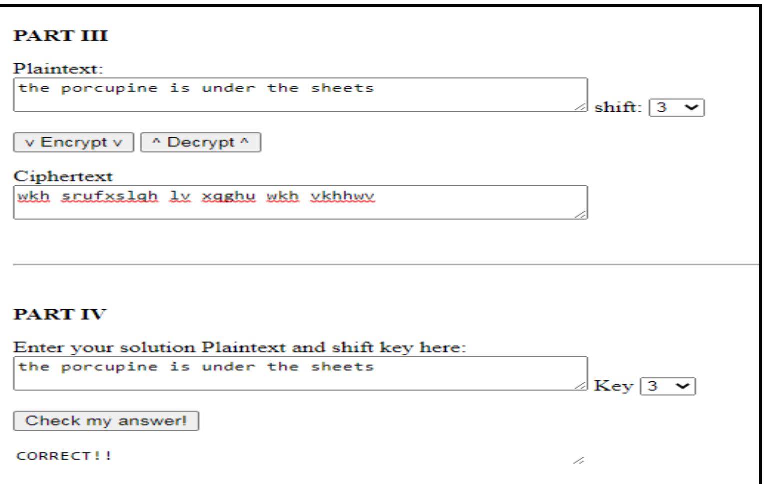
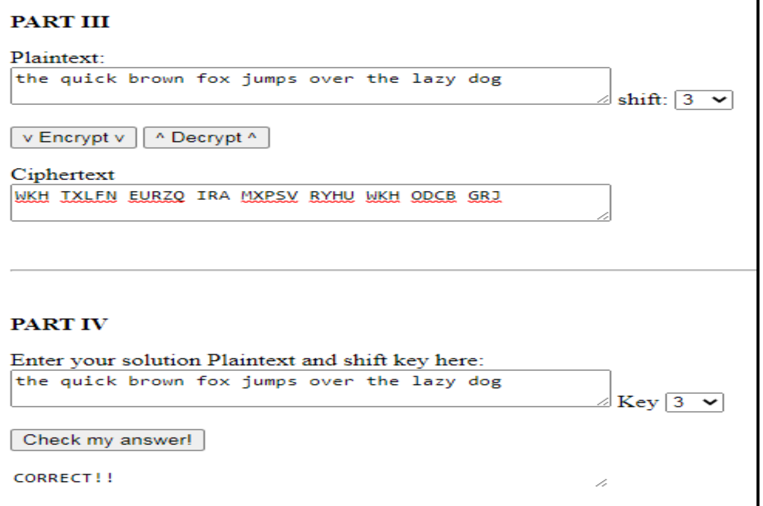
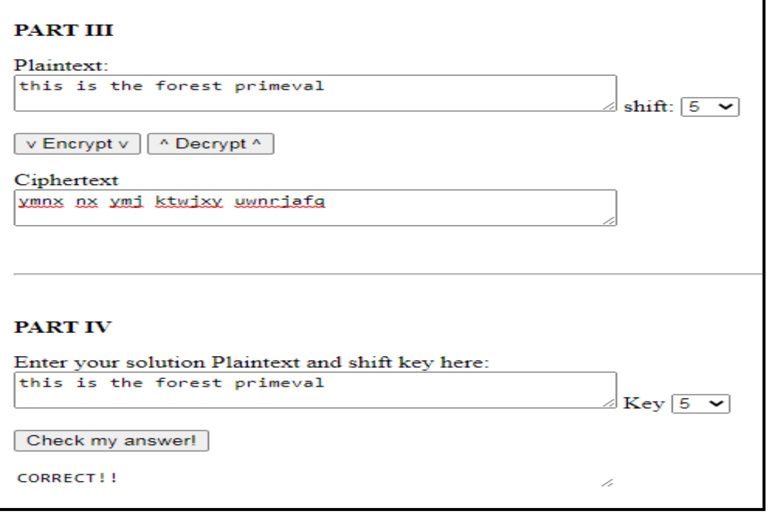
4. **Pattern Matching**:

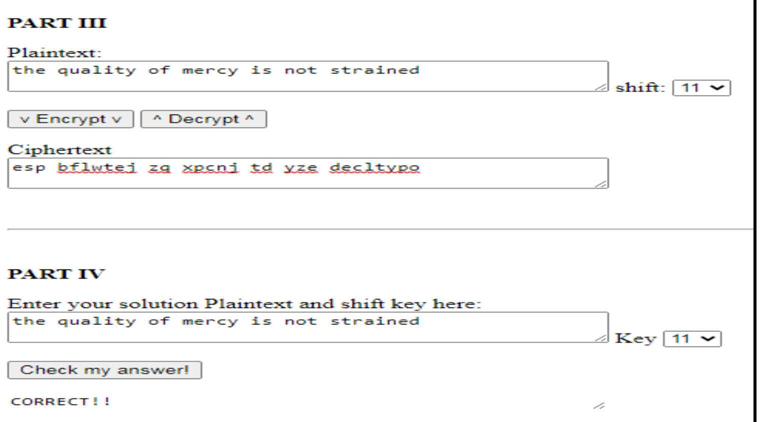
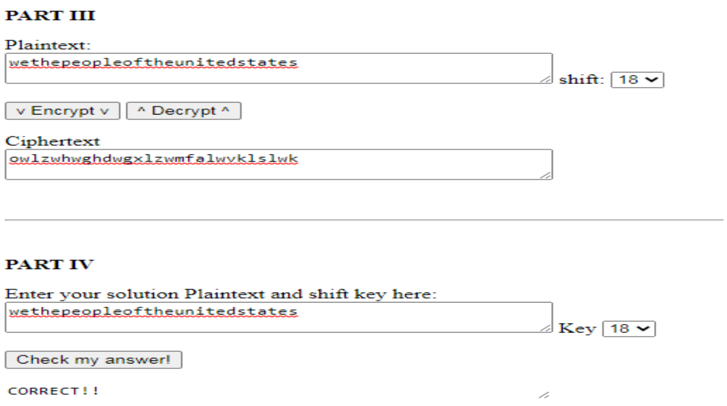
- Look for common patterns (like "TH", "ING") to help identify the shift.

5. **Tools**:

- Use online tools to automate decryption via brute-force or frequency analysis.

Ciphertext	Key	Plaintext	Performance (Virtual Lab)
haahjr ha khdu	7	attack at dawn	 PART III Plaintext: attack at dawn shift: 7 Ciphertext haahjr ha khdu PART IV Enter your solution Plaintext and shift key here: attack at dawn Key 7 CORRECT!!

wkh srukxslqh lv xqghu wkh vkhhwv	3	the porcupine is under the sheets	 PART III Plaintext: the porcupine is under the sheets shift: 3 v Encrypt v ^ Decrypt ^ Ciphertext wkh srufxslqh lv xqghu wkh vkhhwv PART IV Enter your solution Plaintext and shift key here: the porcupine is under the sheets Key 3 Check my answer! CORRECT!!
wkh txlfn eurzo ira mxpsv rhyhu wkh odcb grj	3	the quick brown fox jumps over the lazy dog	 PART III Plaintext: the quick brown fox jumps over the lazy dog shift: 3 v Encrypt v ^ Decrypt ^ Ciphertext WKH TXLFN EURZQ IRA MXPSV RYHU WKH ODCB GRJ PART IV Enter your solution Plaintext and shift key here: the quick brown fox jumps over the lazy dog Key 3 Check my answer! CORRECT!!
ymnx nx ktwjxy uwnrjafq	5	this is the forest primeval	 PART III Plaintext: this is the forest primeval shift: 5 v Encrypt v ^ Decrypt ^ Ciphertext ymnx nx ymj ktwjxy uwnrjafq PART IV Enter your solution Plaintext and shift key here: this is the forest primeval Key 5 Check my answer! CORRECT!!

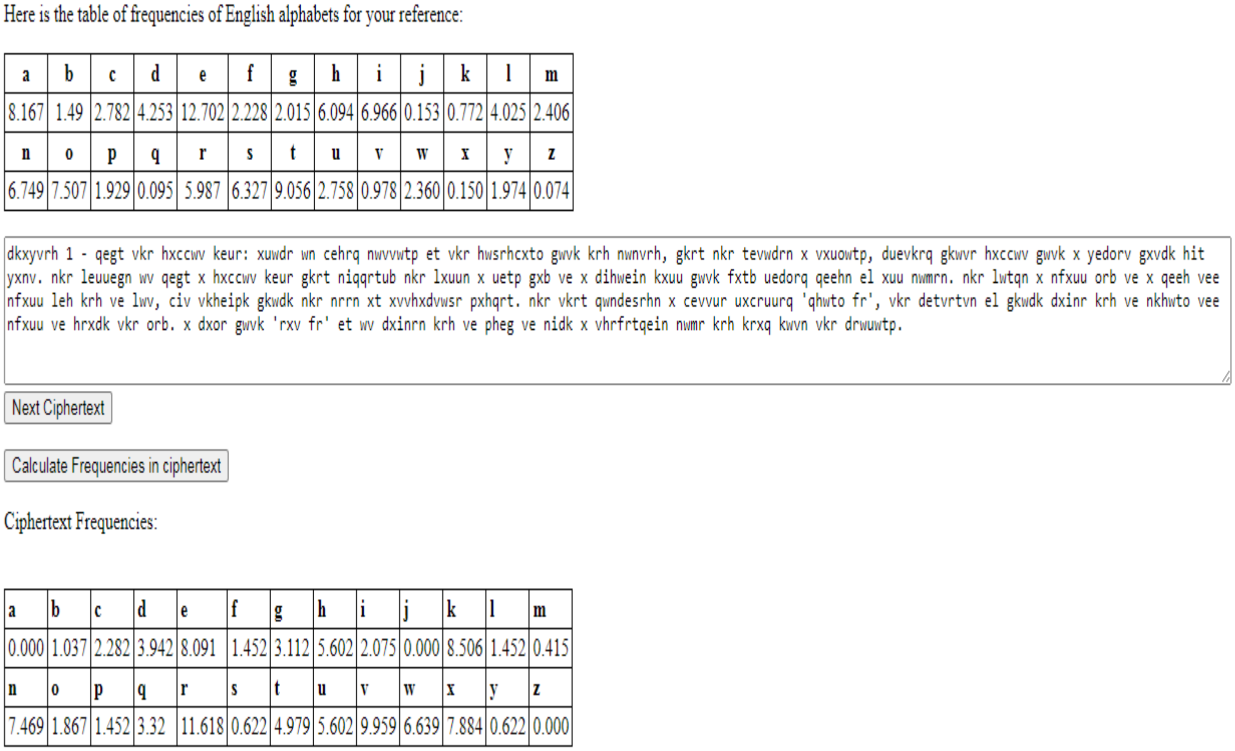
esp bflwtej zq xpcnj td yze decltypo	11	the quality of mercy is not strained	 PART III Plaintext: the quality of mercy is not strained shift: 11 Ciphertext esp bflwtej zq xpcnj td yze decltypo PART IV Enter your solution Plaintext and shift key here: the quality of mercy is not strained Key 11 CORRECT!!
owlzwhwghdw gxlzwmfalwykl slwk	18	Wethepeopl eoftheunited states	 PART III Plaintext: wethepeopleoftheunitedstates shift: 18 Ciphertext owlzwhwghdwgxlzwmfalwvklslwk PART IV Enter your solution Plaintext and shift key here: wethepeopleoftheunitedstates Key 18 CORRECT!!

❖ <u>BREAKING THE MONO-ALPHABETIC SUBSTITUTION CIPHER :</u>

1. **Frequency Analysis**:
- Compare letter frequencies in the ciphertext to the standard letter frequency in English. Common letters like 'E', 'T', 'A' help identify substitutions.
2. **Identify Common Words**:
- Look for common short words like "the", "and", or "is". Substituting letters based on these guesses helps crack other parts of the text.
3. **Pattern Matching**:
- Use letter patterns in common words (e.g., 'TH', 'ING') to guide letter substitutions.
4. **Trial and Error**:
- Gradually replace letters based on frequency and pattern guesses, then check for readable text.
5. **Use Tools**:
    - Software tools can automate frequency analysis and pattern recognition to speed up the decryption process.

PART I

Decrypt the following cipher text. A tool to stimulate the Mono-alphabetic Substitution cipher is provided beneath for your assistance .



Here is the table of frequencies of English alphabets for your reference:

a	b	c	d	e	f	g	h	i	j	k	l	m
8.167	1.49	2.782	4.253	12.702	2.228	2.015	6.094	6.966	0.153	0.772	4.025	2.406
n	**o**	**p**	**q**	**r**	**s**	**t**	**u**	**v**	**w**	**x**	**y**	**z**
6.749	7.507	1.929	0.095	5.987	6.327	9.056	2.758	0.978	2.360	0.150	1.974	0.074

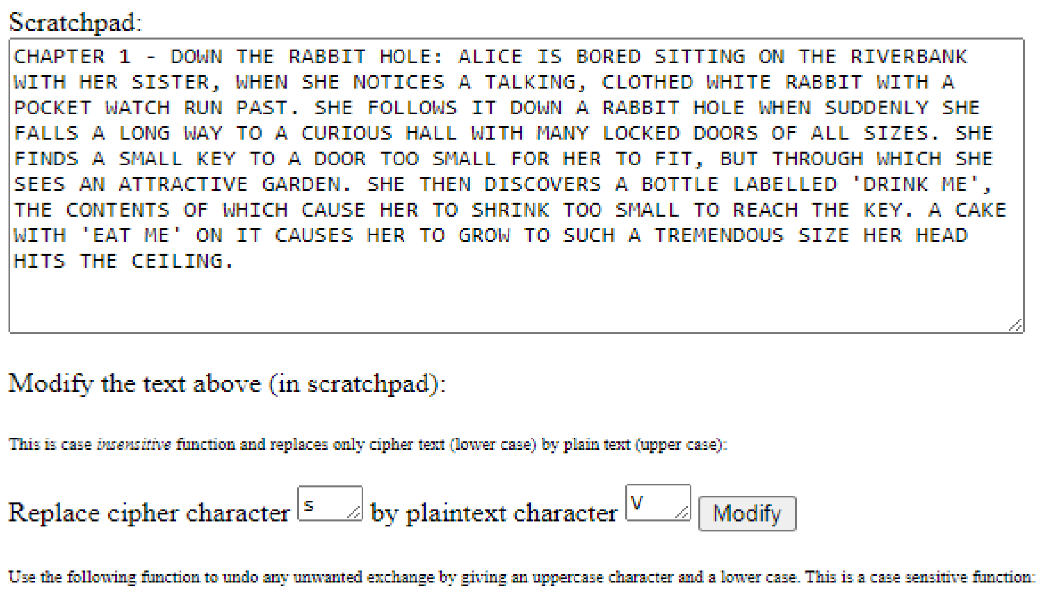
```
dkxyvrh 1 - qegt vkr hxccwv keur: xuwdr wn cehrq nwvvwtp et vkr hwsrhcxto gwvk krh nwnvrh, gkrt nkr tevwdrn x vxuowtp, duevkrq gkwvr hxccwv gwvk x yedorv gxvdk hit
yxnv. nkr leuuegn wv qegt x hxccwv keur gkrt niqqrtub nkr lxuun x uetp gxb ve x dihwein kxuu gwvk fxtb uedorq qeehn el xuu nwmrn. nkr lwtqn x nfxuu orb ve x qeeh vee
nfxuu leh krh ve lwv, civ vkheipk gkwdk nkr nrrn xt xvvhxdvwsr pxhqrt. nkr vkrt qwndesrhn x cevvur uxcruurq 'qhwto fr', vkr detvrtvn el gkwdk dxinr krh ve nkhwto vee
nfxuu ve hrxdk vkr orb. x dxor gwvk 'rxv fr' et wv dxinrn krh ve pheg ve nidk x vhrfrtqein nwmr krh krxq kwvn vkr drwuwtp.
```

Ciphertext Frequencies:

a	b	c	d	e	f	g	h	i	j	k	l	m
0.000	1.037	2.282	3.942	8.091	1.452	3.112	5.602	2.075	0.000	8.506	1.452	0.415
n	o	p	q	r	s	t	u	v	w	x	y	z
7.469	1.867	1.452	3.32	11.618	0.622	4.979	5.602	9.959	6.639	7.884	0.622	0.000

PART II

Note that the cipher text is in lower case and when you replace any character, the final character of replacement, i.e., plaintext is changed to upper case automatically in the following scratchpad.



Scratchpad:

```
CHAPTER 1 - DOWN THE RABBIT HOLE: ALICE IS BORED SITTING ON THE RIVERBANK
WITH HER SISTER, WHEN SHE NOTICES A TALKING, CLOTHED WHITE RABBIT WITH A
POCKET WATCH RUN PAST. SHE FOLLOWS IT DOWN A RABBIT HOLE WHEN SUDDENLY SHE
FALLS A LONG WAY TO A CURIOUS HALL WITH MANY LOCKED DOORS OF ALL SIZES. SHE
FINDS A SMALL KEY TO A DOOR TOO SMALL FOR HER TO FIT, BUT THROUGH WHICH SHE
SEES AN ATTRACTIVE GARDEN. SHE THEN DISCOVERS A BOTTLE LABELLED 'DRINK ME',
THE CONTENTS OF WHICH CAUSE HER TO SHRINK TOO SMALL TO REACH THE KEY. A CAKE
WITH 'EAT ME' ON IT CAUSES HER TO GROW TO SUCH A TREMENDOUS SIZE HER HEAD
HITS THE CEILING.
```

Modify the text above (in scratchpad):

This is case *insensitive* function and replaces only cipher text (lower case) by plain text (upper case):

Replace cipher character s by plaintext character V

Use the following function to undo any unwanted exchange by giving an uppercase character and a lower case. This is a case sensitive function:

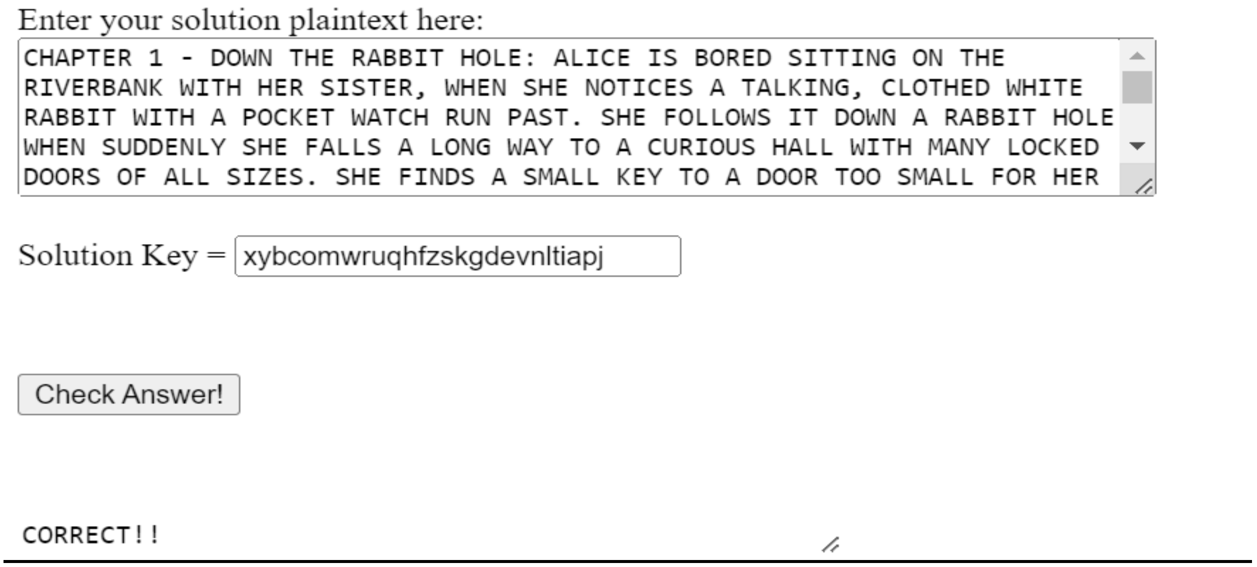
Replacement History :

CIPHERTEXT ALPHABET	PLAINTEXT ALPHABET
a	X
b	Y
c	B
d	C
e	O
f	M
g	W
h	R
i	U
j	Q
k	H
l	F
m	Z
n	S
o	K

p	G
q	D
r	E
s	V
t	N
u	L
v	T
w	I
x	A
y	P
z	J

PART III

Enter the replacement history as your key and verify your answer



Enter your solution plaintext here:

CHAPTER 1 - DOWN THE RABBIT HOLE: ALICE IS BORED SITTING ON THE RIVERBANK WITH HER SISTER, WHEN SHE NOTICES A TALKING, CLOTHED WHITE RABBIT WITH A POCKET WATCH RUN PAST. SHE FOLLOWS IT DOWN A RABBIT HOLE WHEN SUDDENLY SHE FALLS A LONG WAY TO A CURIOUS HALL WITH MANY LOCKED DOORS OF ALL SIZES. SHE FINDS A SMALL KEY TO A DOOR TOO SMALL FOR HER

Solution Key = xybcomwruqhfzskgdevnltiapj

CORRECT!!

CONCLUSION :

Both ciphers can be broken using analysis and logical techniques. The Shift Cipher, being simpler, can be easily cracked through brute-force, frequency analysis, or known plaintext methods. The Mono-Alphabetic Substitution Cipher, though more complex, can still be deciphered using frequency analysis, word patterns, and gradual substitutions. In both cases, the use of software tools can greatly speed up the decryption process. Thus, while different in complexity, both ciphers can be systematically broken using analytical approaches.