



Mahavir Education Trust's
**SHAH & ANCHOR KUTCHHI ENGINEERING
COLLEGE**
Chembur, Mumbai - 400 088
UG Program in Information Technology

Experiment No:1				
Date of Performance:	10-07-24			
Date of Submission:	17-07-24			
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 :

Ciphertext	Key	Plaintext	Performance (Virtual Lab)
haahjr ha khdu	7	attack at dawn	<p>PART III</p> <p>Plaintext: <input type="text" value="attack at dawn"/> shift: <input type="text" value="7"/></p> <p><input type="button" value="v Encrypt v"/> <input type="button" value="^ Decrypt ^"/></p> <p>Ciphertext <input type="text" value="haahjr ha khdu"/></p> <hr/> <p>PART IV</p> <p>Enter your solution Plaintext and shift key here: <input type="text" value="attack at dawn"/> Key <input type="text" value="7"/></p> <p><input type="button" value="Check my answer!"/></p> <p>CORRECT!!</p>
wkh sruxslqh lv xqghu wkh vkhhwv	3	the porcupine is under the sheets	<p>PART III</p> <p>Plaintext: <input type="text" value="the porcupine is under the sheets"/> shift: <input type="text" value="3"/></p> <p><input type="button" value="v Encrypt v"/> <input type="button" value="^ Decrypt ^"/></p> <p>Ciphertext <input type="text" value="wkh sruxslqh lv xqghu wkh vkhhwv"/></p> <hr/> <p>PART IV</p> <p>Enter your solution Plaintext and shift key here: <input type="text" value="the porcupine is under the sheets"/> Key <input type="text" value="3"/></p> <p><input type="button" value="Check my answer!"/></p> <p>CORRECT!!</p>

wkh txlfn eurzo ira mxpsv rhyhu wkh odcB grj	3	the quick brown fox jumps over the lazy dog	<p>PART III</p> <p>Plaintext: the quick brown fox jumps over the lazy dog</p> <p>shift: 3 ▼</p> <p>▼ Encrypt ▼ ^ Decrypt ^</p> <p>Ciphertext WKH TXLFN EURZO IRA MXPSV RYHU WKH ODCB GRJ</p> <hr/> <p>PART IV</p> <p>Enter your solution Plaintext and shift key here: the quick brown fox jumps over the lazy dog</p> <p>Key 3 ▼</p> <p>Check my answer!</p> <p>CORRECT!!</p>
ymnx nx ktwjxy uwnrjafq	5	this is the forest primeval	<p>PART III</p> <p>Plaintext: this is the forest primeval</p> <p>shift: 5 ▼</p> <p>▼ Encrypt ▼ ^ Decrypt ^</p> <p>Ciphertext ymnx nx ymi ktwjxy uwnrjafq</p> <hr/> <p>PART IV</p> <p>Enter your solution Plaintext and shift key here: this is the forest primeval</p> <p>Key 5 ▼</p> <p>Check my answer!</p> <p>CORRECT!!</p>
esp bflwtej zq xpcnj td yze decltypo	11	the quality of mercy is not strained	<p>PART III</p> <p>Plaintext: the quality of mercy is not strained</p> <p>shift: 11 ▼</p> <p>▼ Encrypt ▼ ^ Decrypt ^</p> <p>Ciphertext esp bflwtej zq xpcnj td yze decltypo</p> <hr/> <p>PART IV</p> <p>Enter your solution Plaintext and shift key here: the quality of mercy is not strained</p> <p>Key 11 ▼</p> <p>Check my answer!</p> <p>CORRECT!!</p>

owlzwhwghdw gxlzwmfalwykl slwk	18	Wethepeopl eoftheunited states	PART III Plaintext: <input type="text" value="wethepeopleoftheunitedstates"/> shift: 18 ▼ <input type="button" value="v Encrypt v"/> <input type="button" value="^ Decrypt ^"/> Ciphertext: <input type="text" value="owlzwhwghdwgxlzwmfalwyklslwk"/> <hr/> PART IV Enter your solution Plaintext and shift key here: <input type="text" value="wethepeopleoftheunitedstates"/> Key 18 ▼ <input type="button" value="Check my answer!"/> CORRECT !!
--------------------------------------	----	--------------------------------------	---

❖ BREAKING THE MONO-ALPHABETIC SUBSTITUTION CIPHER :

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 hxcwv keur: xuwr wn cehq nuvvutp et vkr hwsrhcto gwvk krh nwnvrh, gkrt nkr tevdrn x vxuowtp, duevkrq gkivr hxcwv gwvk x yedorv gxvdk hit yxnv. nkr leuegn vv qegt x hxcwv keur gkrt niqrtub nkr lxxun x uetp gxb ve x dihevn kxuu gwvk fxtb uedorq qeehn el xuu nmmrn. nkr lvtqn x nfxuu orb ve x qeeh vee nfxuu leh krh ve luv, civ vkheipk gkwdk nkr nrrn xt xvvhxdvsn pxhqt. nkr vkrt qmndesrh x cevur uxcrurq 'qhwt fr', vkr detvrtvn el gkwdk dxinr krh ve nkhwto vee nfxuu ve hrxdk vkr orb. x dxor gwvk 'rxv fr' et vv dxinn krh ve pheg ve nidk x vhrftrqein nmmr krh krqx kvvn vkr druwutp.

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 by plaintext character

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 =

CORRECT!!

//

