Harsh Mishra
T21-64
Assignment-1

Assignment-1

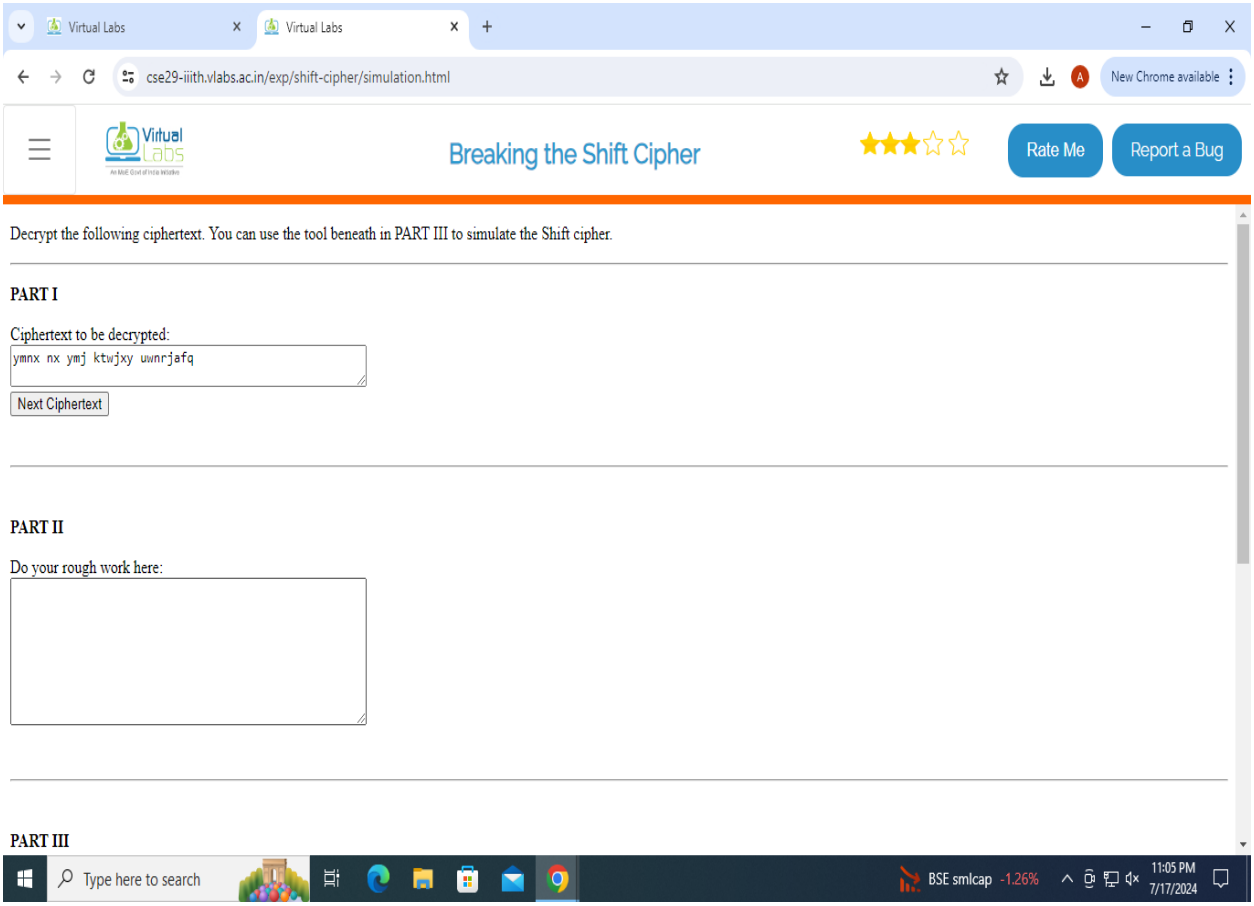
Aim- Illustrate symmetric cryptography by implementing classical ciphers.

Shift Cipher

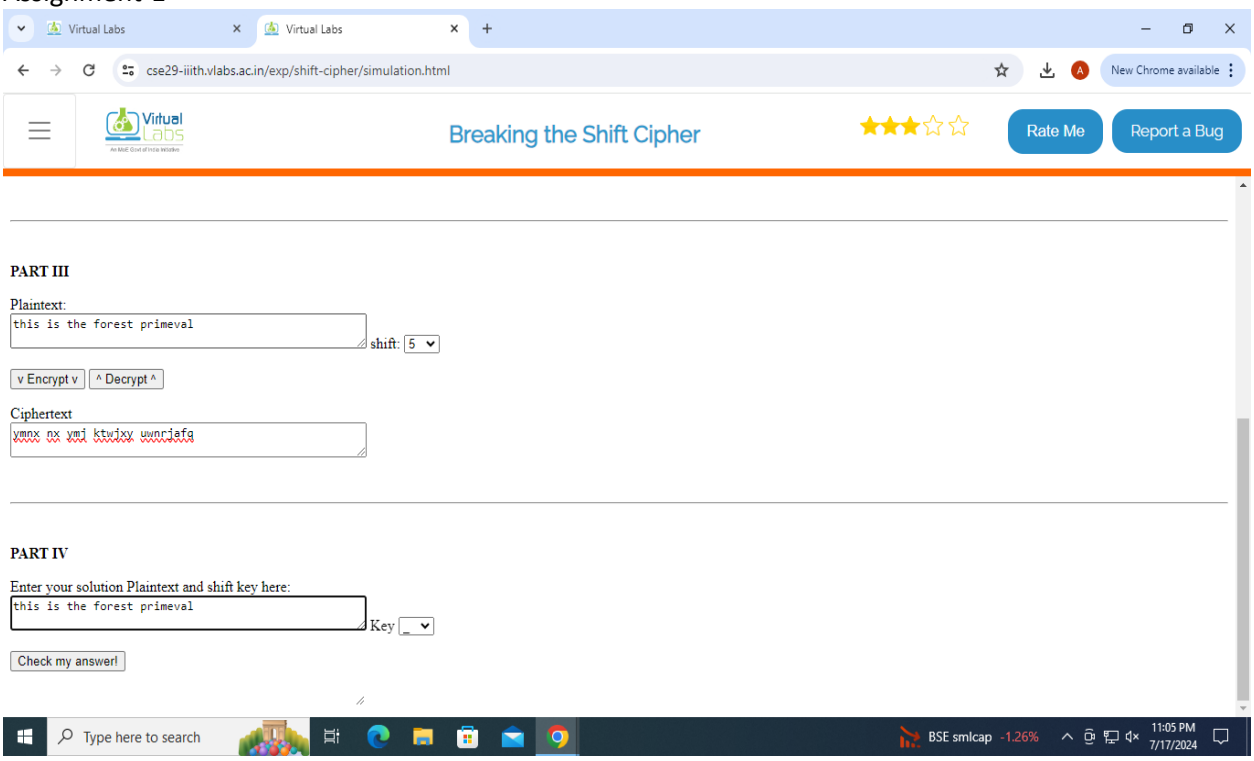
Theory:

A shift cipher, also known as a Caesar cipher, is a type of substitution cipher where each letter in the plaintext is shifted by a fixed number of positions down or up the alphabet. For example, with a shift of 3, the letter 'A' would be replaced by 'D', 'B' by 'E', and so on. After reaching the end of the alphabet, it wraps around, so 'Z' would shift to 'C'. The shift amount serves as the key for both encryption and decryption. This cipher is simple but easy to break due to its limited number of possible shifts.

Implementation:



Harsh Mishra
T21-64
Assignment-1



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!!

Harsh Mishra
T21-64
Assignment-1

Mono-alphabetic Substitution Cipher

Theory:-

A mono alphabetic cipher is a type of substitution cipher where each letter in the plaintext is replaced by a fixed, different letter throughout the entire message. Unlike a shift cipher, where the substitution follows a systematic shift, the substitutions in a mono alphabetic cipher are arbitrary but consistent. For example, 'A' might always be replaced by 'Q', 'B' by 'M', and so on. The key to this cipher is the specific mapping of each letter, making it more secure than a Caesar cipher but still vulnerable to frequency analysis, where common letters and patterns are analyzed to break the code.

Implementation:-

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 SITES. 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 SITE HER HEAD HITS THE CEILING.

PART I

Decrypt the following cipher text. A tool to simulate the Mono-Alphabetic Subsitution 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
```

Next Ciphertext

Calculate Frequencies in ciphertext

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

Harsh Mishra
T21-64
Assignment-1

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
SITES. 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 SITE 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 [m] by plaintext character [t] [Modify]

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

Replace character [M] by character [D] [Replace these exact characters]

Your replacement history:

You replaced d by C You replaced k by H You replaced x by A You replaced y by P You replaced v by T You replaced r by E You replaced h by R You replaced q by M You replaced e by O You replaced q by W You replaced g by W You replaced w by I You replaced n by S You replaced t by N You replaced p by G You replaced M by D You replaced u by L You replaced c by B You replaced l by F You replaced o by K You replaced s by V You replaced i by U You replaced b by Y You replaced f by M You replaced m by T