Khushbu Ahuja

T11 Roll no. 02

AIM: To perform decoding of shift cipher and mono alphabet substitution cipher.

THEORY:

Shift Cipher (Caesar Cipher)

The **Shift Cipher**, also known as the **Caesar Cipher**, is one of the simplest and most well-known encryption techniques. It is a type of substitution cipher where each letter in the plaintext is shifted by a certain number of places down or up the alphabet. The key in a shift cipher is the number of positions each letter is shifted.

How it Works:

1. **Encryption**:
   - Choose a shift value (e.g., 3).
   - For each letter in the plaintext, find its position in the alphabet. ○ Shift it by the chosen value and replace it with the resulting letter.
   - If the shift moves past the end of the alphabet, it wraps around to the beginning. ○ Example: With a shift of 3, "A" becomes "D", "B" becomes "E", and so on.

Ci=(Pi+k)mod 26C_i = (P_i + k) \mod 26Ci=(Pi+k)mod26

Where CiC_iCi is the i-th character of the ciphertext, PiP_iPi is the i-th character of the plaintext, and kkk is the shift key.

2. **Decryption**:
   - Reverse the process by shifting each letter in the ciphertext back by the same number of positions. ○ Example: With a shift of 3, "D" becomes "A", "E" becomes "B", and so on.

Pi=(Ci−k)mod 26P_i = (C_i - k) \mod 26Pi=(Ci−k)mod26 **Example:**

- Plaintext: HELLO

- Shift: 3
- Ciphertext: KHOOR

Monoalphabetic Substitution Cipher

A **Monoalphabetic Substitution Cipher** is a more general form of substitution cipher where each letter in the plaintext is replaced by a corresponding letter in the ciphertext. However, unlike the Caesar Cipher, the substitution is not necessarily a fixed shift; instead, any permutation of the alphabet can be used as the key.

How it Works:

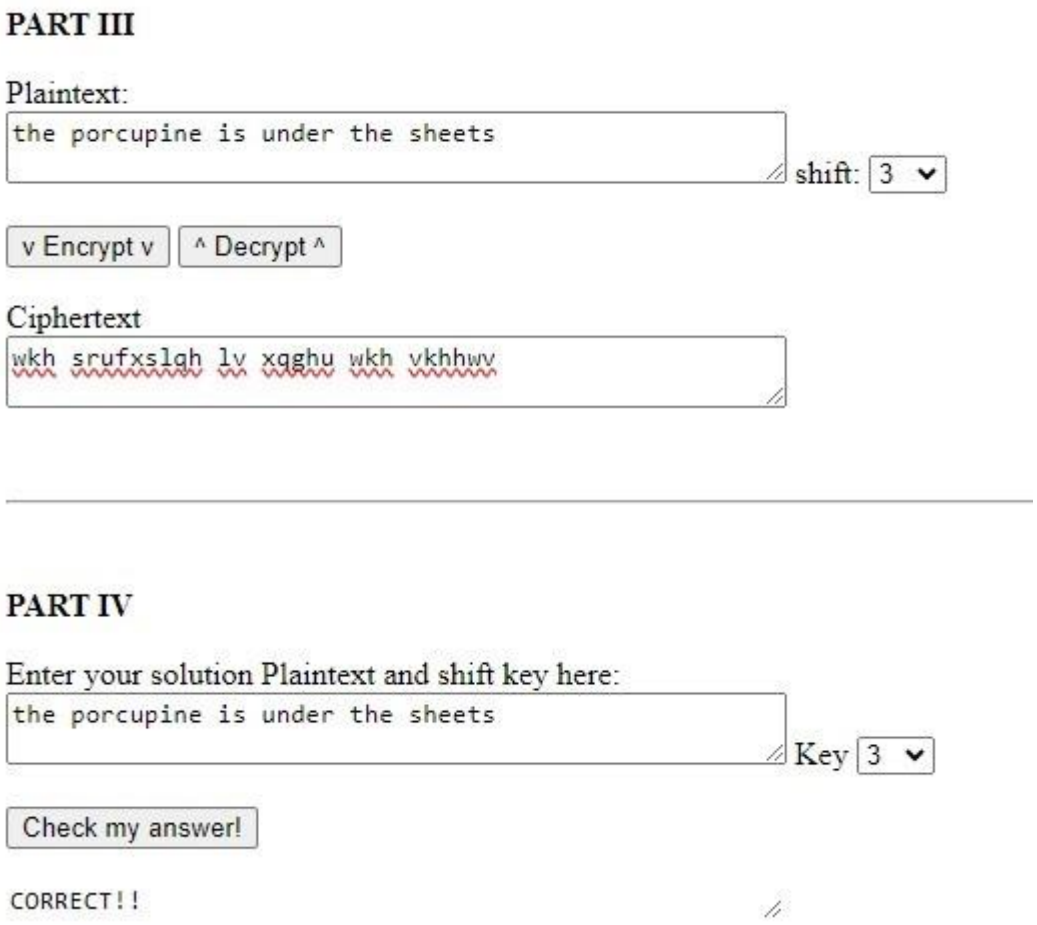
1. **Key Generation**:
    - Create a random permutation of the alphabet. This permutation will serve as the key.
    - Example key: QWERTYUIOPLKJHGFDSAZXCVBNM
    - Each letter of the plaintext is substituted with the corresponding letter from the key.
2. **Encryption**:
    - For each letter in the plaintext, find its position in the regular alphabet. ○ Replace it with the letter in the same position in the substitution key. ○ Example: With the above key, "A" would be replaced by "Q", "B" by "W", etc.
3. **Decryption**:
    - Reverse the process by substituting each letter in the ciphertext with the corresponding letter in the regular alphabet. ○ Example: With the above key, "Q" would be replaced by "A", "W" by "B", etc.

Example:

- Plaintext: HELLO
- Key: QWERTYUIOPLKJHGFDSAZXCVBNM
- Ciphertext: ITSSG

IMPLEMENTATION:

(SHIFT CIPHER)



PART III

Plaintext:

the porcupine is under the sheets

shift: 3

Ciphertext

wkh srufxslqh lv xqghu wkh vkhhwv

PART IV

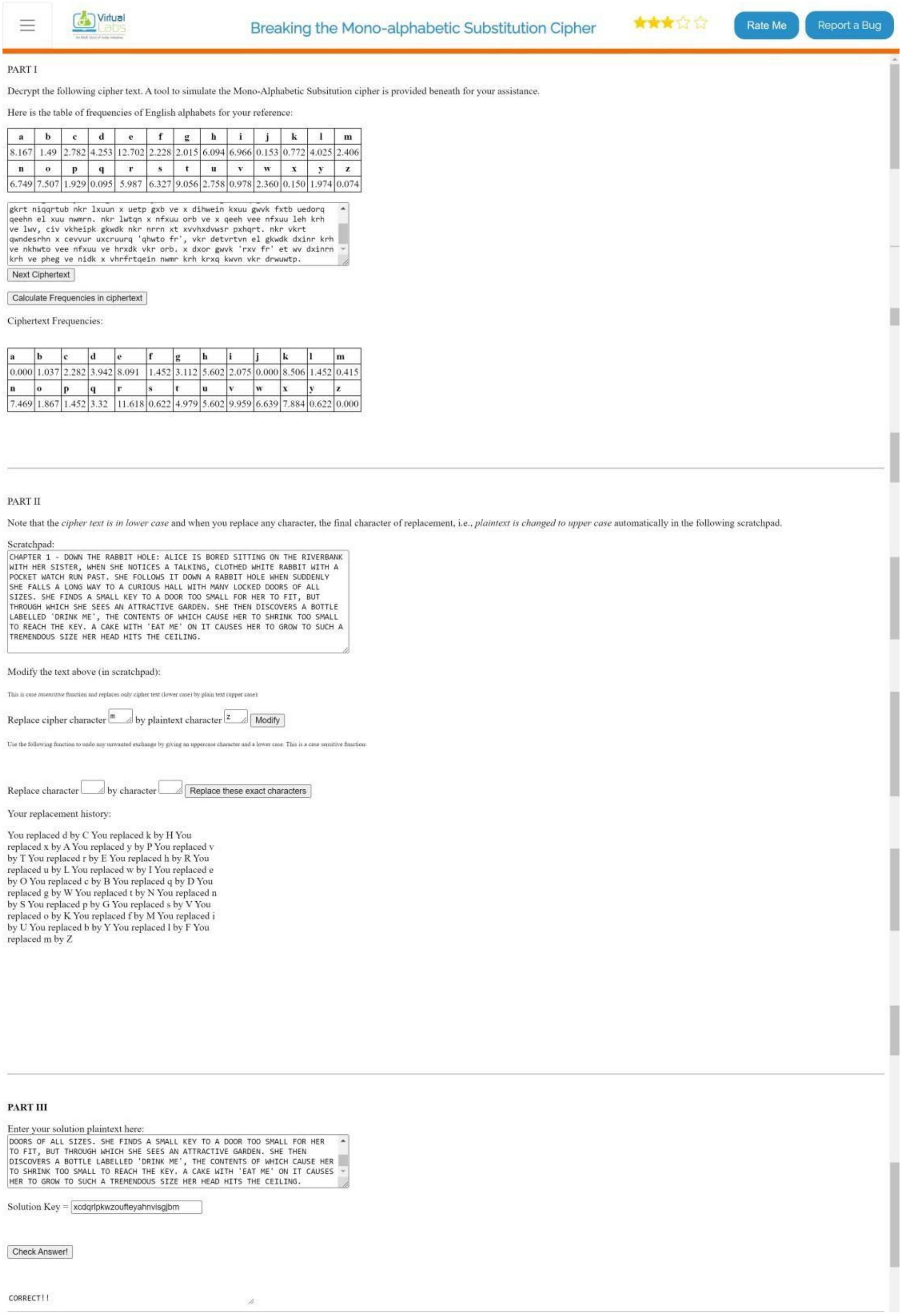
Enter your solution Plaintext and shift key here:

the porcupine is under the sheets

Key 3

CORRECT!!

(MONO ALPHABETIC CIPHER)



Breaking the Mono-alphabetic Substitution Cipher

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

```
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.
```

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

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 m by plaintext character z 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 by character 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 u by L You replaced w by I You replaced e by O You replaced c by B You replaced q by D You replaced g by W You replaced t by N You replaced n by S You replaced p by G You replaced s by V You replaced o by K You replaced f by M You replaced i by U You replaced b by Y You replaced l by F You replaced m by Z

PART III

Enter your solution plaintext here:

```
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.
```

Solution Key = xcdqrlpkwzoufteyahnvisgjbm

Check Answer!

```
CORRECT!!
```

CONCLUSION: Successfully performed decoding of shift cipher and mono alphabet substitution cipher.