Roll No: 09
Name: Shreya Bagade
Date: 21/07/2023

LAB ASSIGNMENT NO:01

Aim: Breaking Shift Cipher and Mono-alphabetic Substitution Cipher using Frequency analysis method.

Lab Outcome Attained: Illustrate symmetric cryptography by implementing classical ciphers.

Theory:

What is shift cipher?

A shift cipher, also known as a Caesar cipher, is a simple form of encryption technique where each letter in the plaintext is replaced by a letter that is a fixed number of positions down the alphabet. The "shift" refers to the number of positions each letter is moved.

Example- Plaintext: HELLO

Choose a shift value (in this case- 3).

Encryption: Each letter is shifted three positions down the alphabet.

H -> K

E -> H

L -> O

L -> O

O -> R

Ciphertext: KHOOR

In this example, the word "HELLO" is encrypted into "KHOOR" using a shift of 3. To decrypt the message, you would apply the opposite shift (in this case, a shift of -3) to each letter in the ciphertext, moving them back up the alphabet to reveal the original plaintext.

How and why, it can be broken using brute force attack?

A shift cipher is relatively simple, and the key space (possible keys) is small since there are only 26 possible shifts (assuming we are dealing with the English alphabet). As a result, a brute force attack becomes a viable method to break the shift cipher.

A brute force attack involves trying all possible combinations of the encryption key until the correct one is found. In the case of a shift cipher, this means trying all 26 possible shifts. The attacker would decrypt the ciphertext using each shift and examine the resulting plaintext to see if it looks like a valid message in English. The correct key is the one that produces a meaningful message.

What is Mono-alphabetic cipher?

A monoalphabetic cipher is a type of substitution cipher where each letter in the plaintext is consistently replaced by the same corresponding letter or symbol in the ciphertext. In other words, one fixed alphabet is used to encrypt the entire message. It is a straightforward and easily understandable form of encryption.

The relationship between a character in the plain text and the characters in the cipher text is one-to-one. Each alphabetic character of plain text is mapped onto a unique alphabetic character of a cipher text.

Example- Plaintext: HELLO

Key: ABCDEFGHIJKLMNOPQRSTUVWXYZ

Cipher: KLMNO

In this example, the letters in the plaintext "HELLO" are replaced according to the key. The letter "H" is replaced by "K," "E" is replaced by "L," and so on. The resulting ciphertext is "KLMNO."

It's essential to note that the key must consist of all 26 letters of the alphabet, and each letter can only appear once in the key to maintain the one-to-one correspondence.

How and why, it can be broken using brute force attack?

A monoalphabetic cipher can be broken using a brute force attack due to its limited key space. Since each letter in the plaintext is consistently replaced by the same corresponding letter or symbol in the ciphertext, the key space is the total number of possible arrangements of the 26 letters of the alphabet.

The number of possible keys for a monoalphabetic cipher is 26, which is approximately 4 x 10^26. While this might seem large at first glance, modern computers can perform a vast number of calculations per second, making a brute force attack feasible.

How it can be broken using frequency analysis attack?

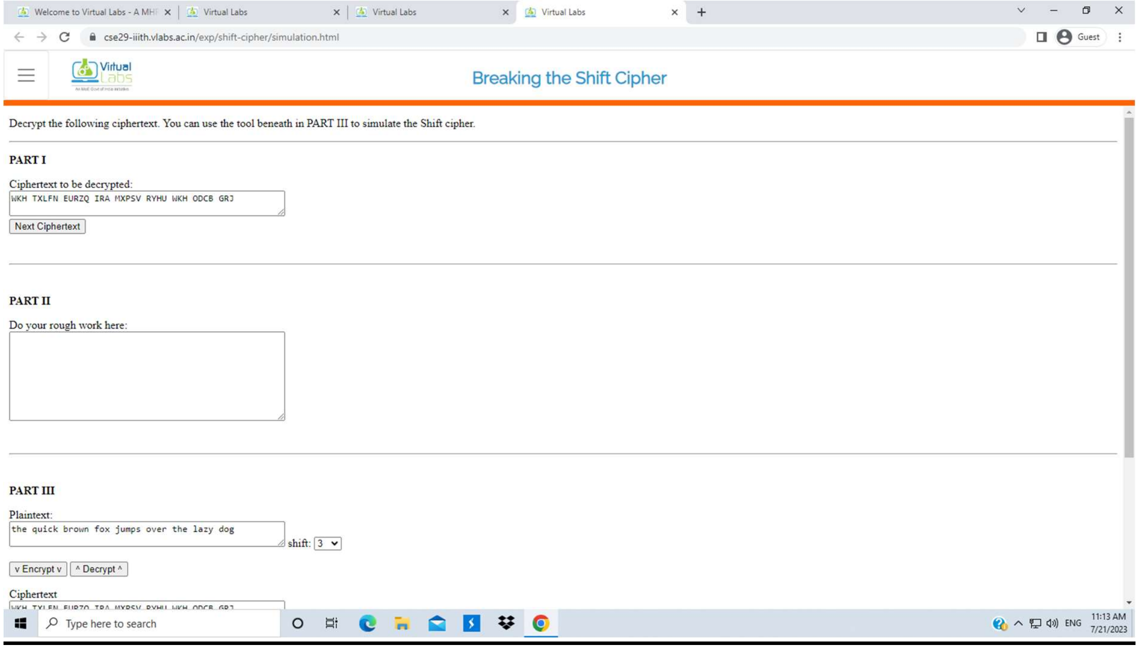
A monoalphabetic cipher can be broken using a frequency analysis attack due to the predictable patterns it creates in the ciphertext. In this type of cipher, each letter in the plaintext is consistently replaced by the same corresponding letter or symbol in the ciphertext. As a result, the frequency distribution of letters in the ciphertext reflects the frequency distribution of the original plaintext, making certain letters more likely to represent specific letters in the original message.

Here's how a frequency analysis attack works:

1. Collect Ciphertext: The attacker obtains the ciphertext, which is the encrypted message.
2. Analyse Letter Frequencies: The attacker calculates the frequency of each letter in the ciphertext. For example, they may find that certain ciphertext letters occur more frequently than others.
3. Compare with Expected Frequency Distribution: In the English language, certain letters occur with higher frequency. For instance, 'E' is the most common letter, followed by 'T,' 'A,' 'O,' 'I,' etc. The attacker compares the frequency distribution of letters in the ciphertext with the expected frequency distribution of letters in English.
4. Guessing the Key: The attacker makes educated guesses about which ciphertext letters correspond to the most frequently occurring letters in English. For example, if 'Z' appears most frequently in the ciphertext, the attacker might assume it represents 'E.'
5. Test the Key: The attacker uses their guess for the mapping of letters as a potential key to decrypt the ciphertext.
6. Validate the Decryption: The attacker examines the resulting plaintext to see if it makes sense. They look for common English words and patterns to confirm that their guess for the key is correct.
7. Iterate and Refine: If the decryption does not produce a sensible message, the attacker repeats steps 4 to 6 with different assumptions until they find a key that successfully decrypts the ciphertext into a coherent English message.

Frequency analysis is effective against monoalphabetic ciphers because the fixed substitution pattern creates regularities in the ciphertext that correspond to the language's letter frequency. However, frequency analysis is not effective against more complex encryption techniques, such as polyalphabetic ciphers or modern encryption algorithms, which use multiple alphabets or involve more sophisticated encryption operations to break the frequency patterns.

Output Screenshots:



Breaking the Shift Cipher

Decrypt the following ciphertext. You can use the tool beneath in PART III to simulate the Shift cipher.

PART I

Ciphertext to be decrypted:

```
WKH TXLFN EURZQ IRA MXPSV RYHU WKH ODCB GRJ
```

Next Ciphertext

PART II

Do your rough work here:

PART III

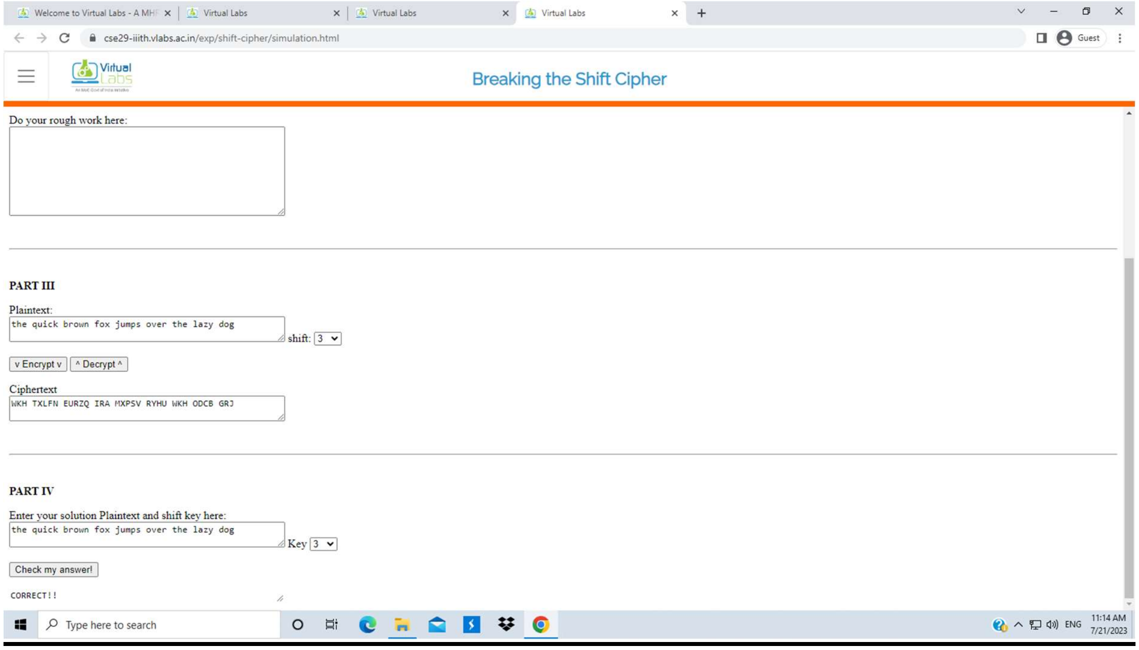
Plaintext:

```
the quick brown fox jumps over the lazy dog
```

shift: 3

v Encrypt v   ^ Decrypt ^

Ciphertext



Breaking the Shift Cipher

Do your rough work here:

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:

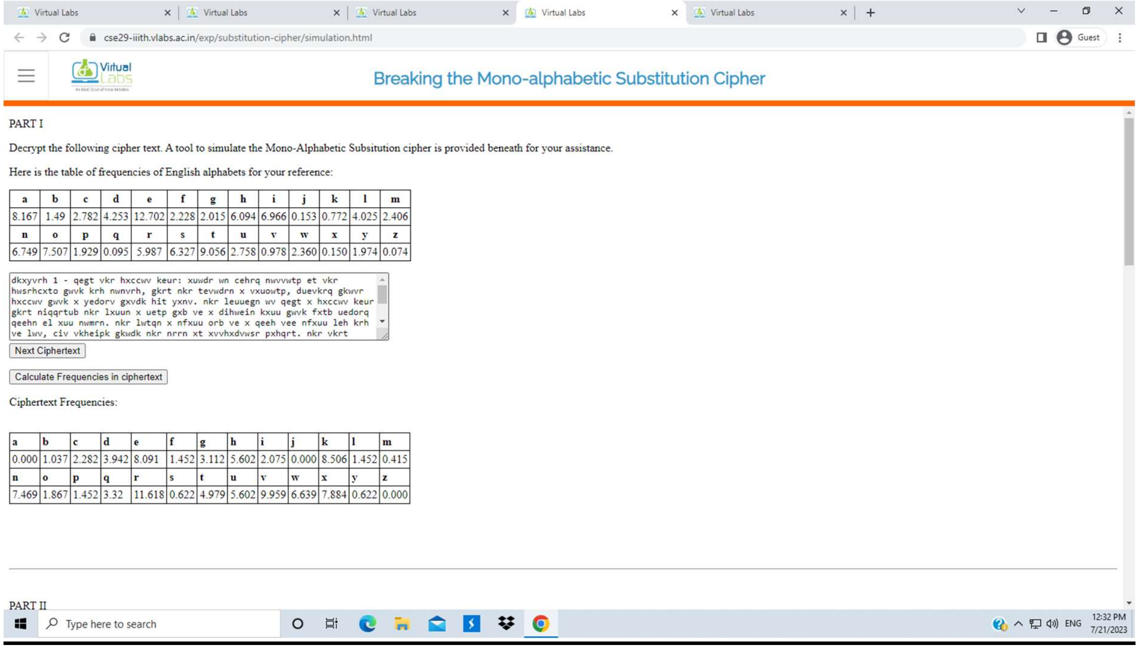
```
the quick brown fox jumps over the lazy dog
```

Key 3

Check my answer!

```
CORRECT!!
```

Roll No: 09
Name: Shreya Bagade
Date: 21/07/2023



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

```
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
```

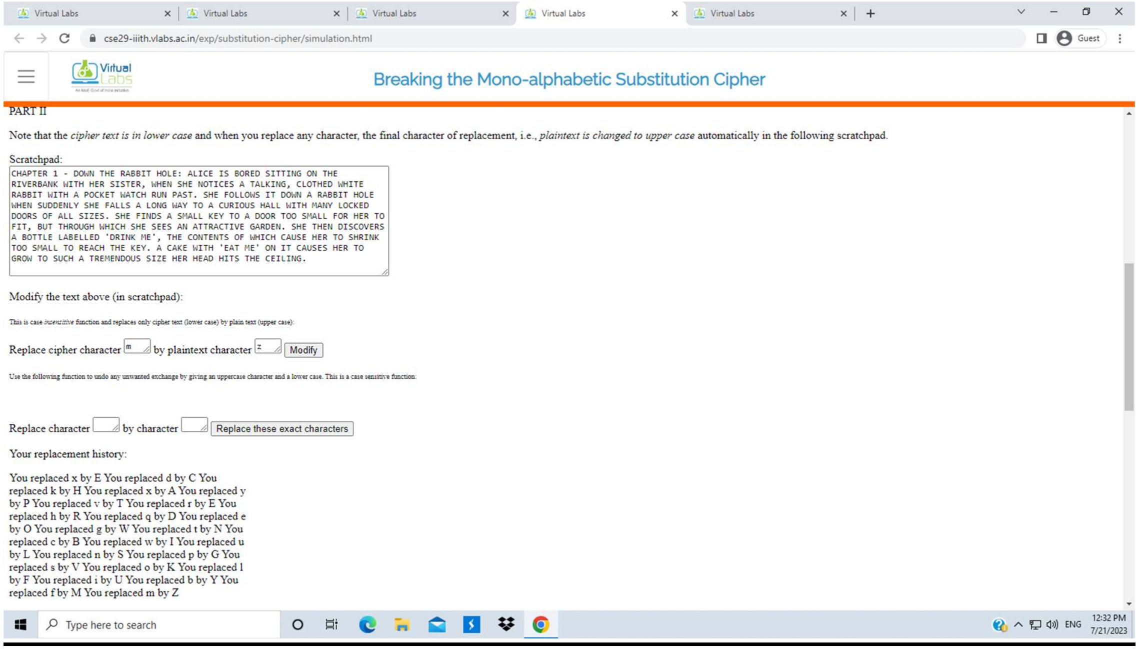
Next Ciphertext

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



Breaking the Mono-alphabetic Substitution Cipher

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

Conclusion: We learnt about Shift cipher and Mono-alphabetic substitution cipher and their fundamentals in terms of security. The shift cipher, also known as the Caesar cipher, relies on a fixed shift value, whereas in monoalphabetic substitution cipher, plain text is mapped to a fixed symbol in cipher text. It is slightly more complex, remains vulnerable to frequency analysis attacks.