Assignment 1

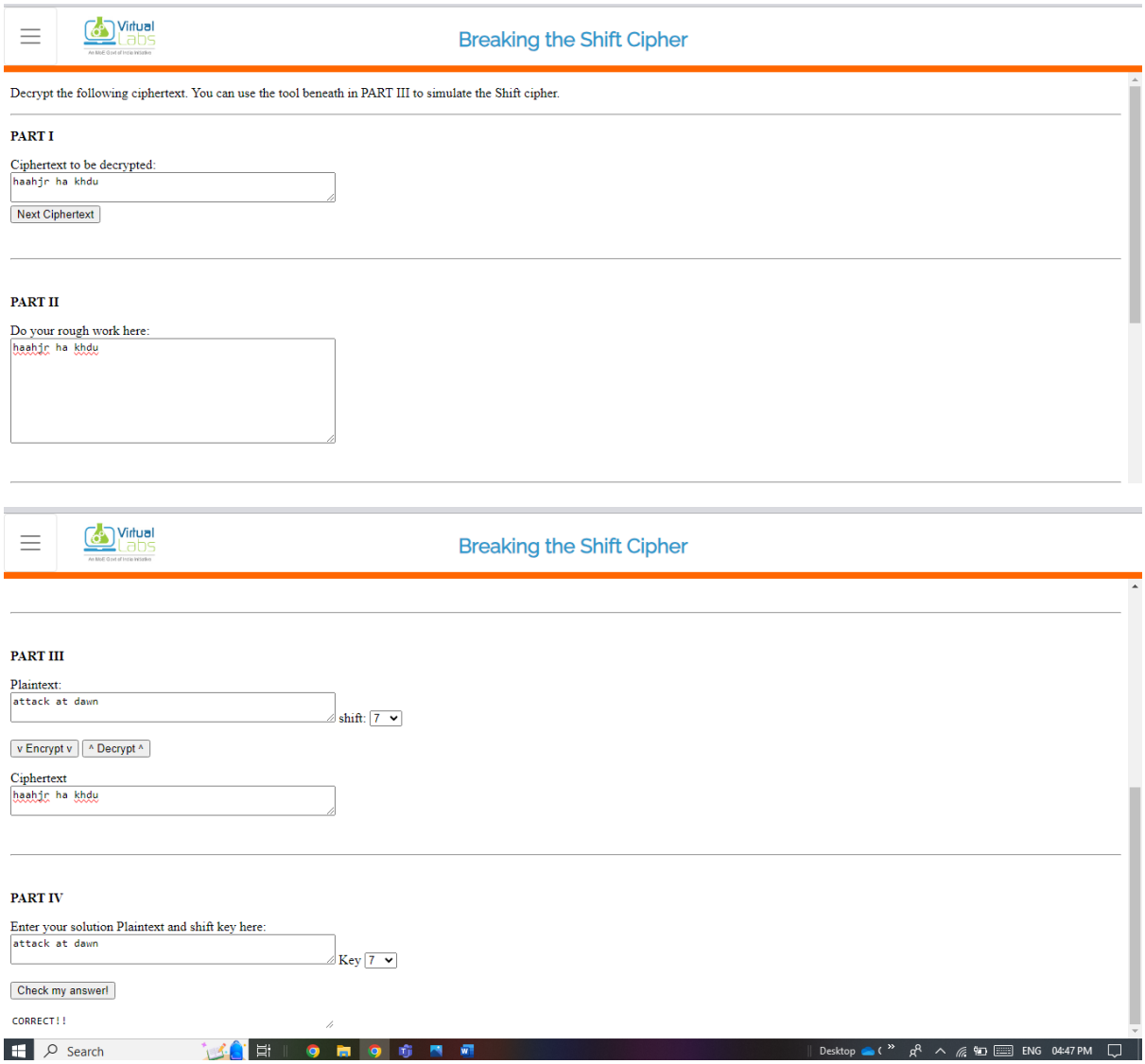
Aim: Breaking shift cipher and Mono-alphabetic Substitution Cipher using Frequency analysis method.

Lab outcome: Illustrate symmetric cryptography by implementing classical ciphers

Theory:

What is shift cipher?

A shift cipher, also known as a Caesar cipher, is a basic and straightforward encryption technique used in cryptography. It is one of the earliest and simplest methods of encryption. In a shift cipher, each letter in the plaintext is shifted a fixed number of positions down or up the alphabet. The number of positions shifted is called the "key" or "shift value." For example, with a shift of 3, "A" would be encrypted as "D," "B" would become "E," and so on. The shift wraps around the alphabet, so "Z" would be encrypted as "C' with a shift of 3.

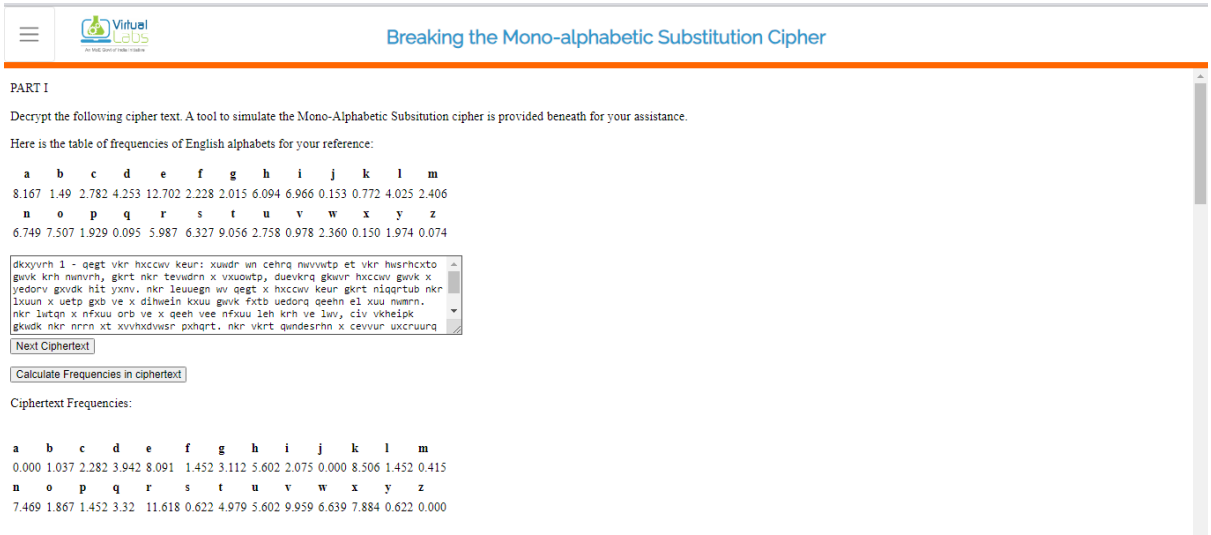


How and why it can be broken using brute force attack?

A shift cipher (Caesar cipher) can be broken using a brute force attack due to its limited key space. Since there are only 26 possible keys in the case of the English alphabet (shifting 0 to 25 positions), an attacker can systematically try all possible keys to decrypt the ciphertext. Here's how a brute force attack works on a shift cipher: Enumerate all possible keys: Since there are only 26 possible keys, the attacker tries all combinations, shifting the ciphertext by 0 to 25 positions. Decrypt the ciphertext: For each key, the attacker shifts the ciphertext letters back by the corresponding number of positions to recover the plaintext. Check for meaningful results: After decrypting with each key, the attacker examines the output to see if it resembles meaningful English text. The assumption is that the correct key will produce a message that is easily recognizable as a coherent sentence or phrase. Verify the result: The attacker usually employs some form of automated or manual analysis to check the output for linguistic patterns, common words, or other recognizable features that indicate a successful decryption. Select the correct key: Once the attacker finds the decryption that appears to be meaningful English text, they have likely found the correct key, and the message is deciphered. The reason a shift cipher is vulnerable to brute force attacks is that it has a very small key space. With only 26 possible keys, trying all combinations is a relatively trivial task for a computer program or a determined attacker. This simplicity is why the shift cipher is considered weak and is not used for secure encryption purposes today.

What is monoalphabetic cipher?

A monoalphabetic cipher is a type of substitution cipher where each letter in the plaintext is replaced with a fixed corresponding letter in the ciphertext. In other words, the same substitution rule is applied consistently throughout the entire message. This means that each occurrence of a specific letter in the plaintext will always be replaced by the same letter in the ciphertext



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 sensitive 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 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 i by U You replaced l by F You replaced b by Y You replaced f by M You replaced m by Z

Virtual Labs

Breaking the Mono-alphabetic Substitution Cipher

PART III

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 = xcdqrlpkwzoufteyahnvisgjbm

Check Answer!

CORRECT!!

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

A shift cipher (Caesar cipher) can be broken using a brute force attack due to its limited key space. Since there are only 26 possible keys in the case of the English alphabet (shifting 0 to 25 positions), an attacker can systematically try all possible keys to decrypt the ciphertext. Here's how a brute force attack works on a shift cipher: Enumerate all possible keys: Since there are only 26 possible keys, the attacker tries all combinations, shifting the ciphertext by 0 to 25 positions. Decrypt the ciphertext: For each key, the attacker shifts the ciphertext letters back by the corresponding number of positions to recover the plaintext. Check for meaningful results: After decrypting with each key, the attacker examines the output to see if it resembles meaningful English text. The assumption is that the correct key will produce a message that is easily recognizable as a coherent sentence or phrase.

Verify the result: The attacker usually employs some form of automated or manual analysis to check the output for linguistic patterns, common words, or other recognizable features that indicate a successful decryption. Select the correct key: Once the attacker finds the decryption that appears to be meaningful English text, they have likely found the correct key, and the message is deciphered.

The reason a shift cipher is vulnerable to brute force attacks is that it has a very small key space. With only 26 possible keys, trying all combinations is a relatively trivial task for a

computer program or a determined attacker. This simplicity is why the shift cipher is considered weak and is not used for secure encryption purposes today.

How it is broken using frequency analysis attack?

Breaking the Caesar cipher is trivial as it is vulnerable to most forms of attack. The system is so easily broken that it is often faster to perform a brute force attack to discover if this cipher is in use or not. An easy way for humans to decipher it is to examine the letter frequencies of the cipher text and see where they match those found in the underlying language.

By graphing the frequencies of letters in the ciphertext and those in the original language of the plaintext, a human can spot the value of the key by looking at the displacement of particular features of the graph. For example in the English language the frequencies of the letters Q,R,S,T have a particularly distinctive pattern.

Conclusion :

We understood the working of shift and monoalphabetic cipher and successfully implemented the simulation of shift and monoalphabetic cipher using virtual lab