Assignment 1

Aim: Breaking Shift Cipher and Monoalphabetic Substitution Cipher using Frequency analysis method

Theory:

Shift Cipher (Caesar Cipher):

The Shift Cipher, also known as the Caesar Cipher, is one of the simplest and most well-known substitution ciphers. It works by shifting each letter in the plaintext by a fixed number of positions in the alphabet. The key in this cipher is the shift value, which determines the amount of the shift.

Encryption:

- Each letter in the plaintext is shifted by a fixed number of positions.
- For example, with a shift of 3: 'A' becomes 'D', 'B' becomes 'E', 'C' becomes 'F', and so on.
- Wraparound occurs at the end of the alphabet. For example, 'X' becomes 'A', 'Y' becomes 'B', and 'Z' becomes 'C'.

Decryption:

- To decrypt, the same shift value is used in the opposite direction.
- For a shift of 3: 'D' becomes 'A', 'E' becomes 'B', 'F' becomes 'C', and so on.

Monoalphabetic Substitution Cipher:

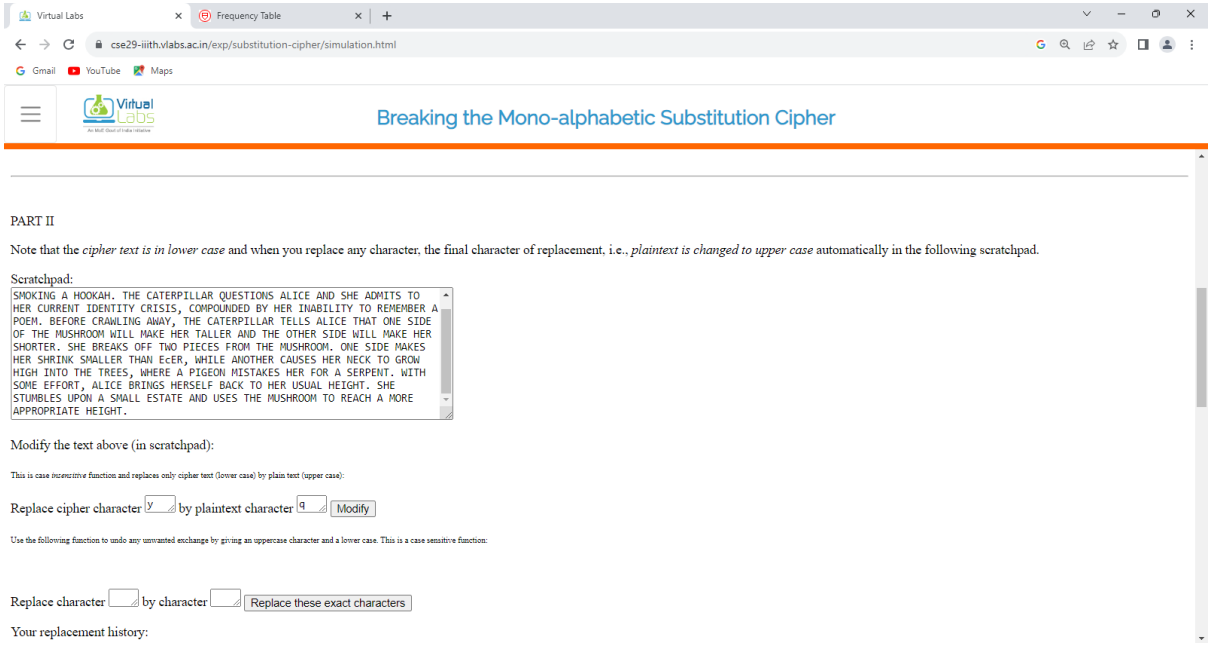
A Monoalphabetic Substitution Cipher is a substitution cipher where each letter in the plaintext is replaced with another letter from a fixed substitution key. Unlike the Shift Cipher, each letter can be replaced by any other letter, making it more secure. However, the key must be kept secret.

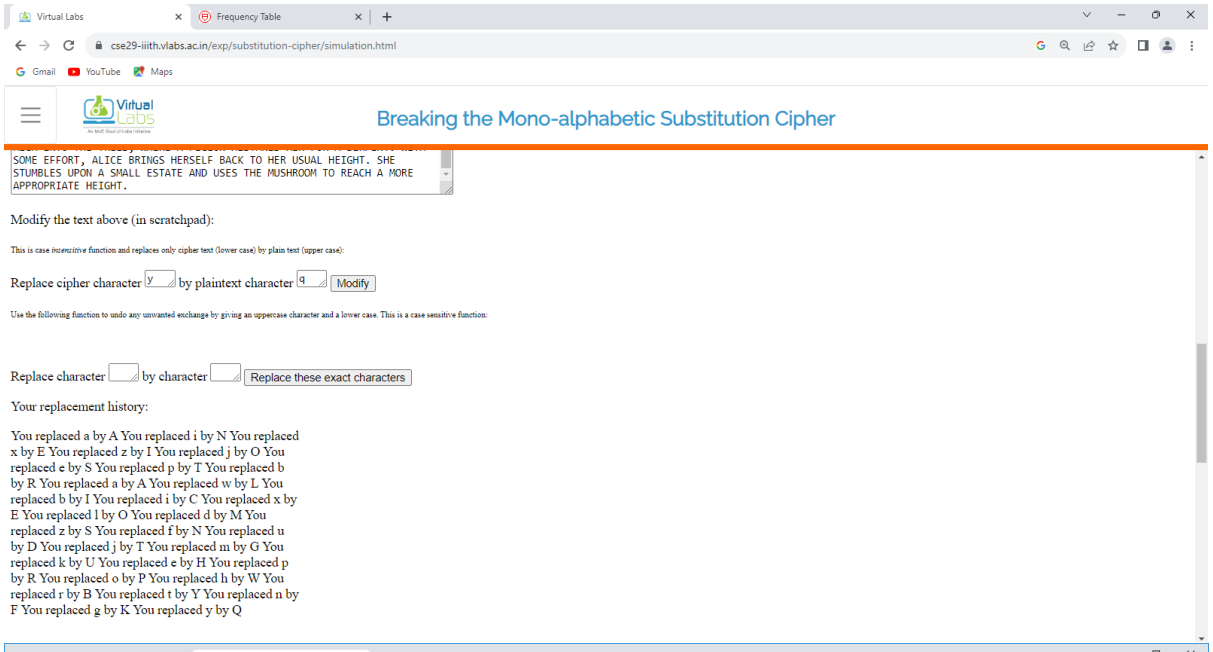
Encryption:

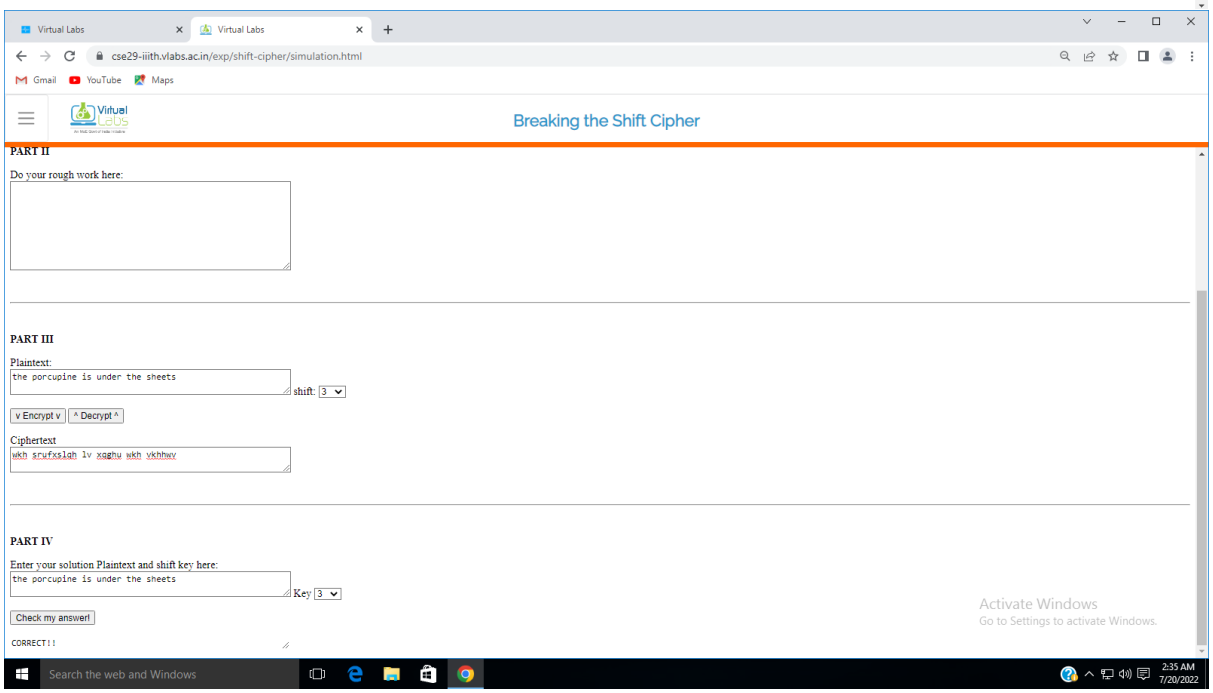
- A key defines the substitution mapping for each letter.
- For example, 'A' might be replaced by 'Q', 'B' by 'Z', and so on.

Decryption:

- The same key is used to reverse the substitution and decrypt the message.


Virtual Labs
Frequency Table
cse29-iiith.vlabs.ac.in/exp/substitution-cipher/simulation.html
Gmail
YouTube
Maps
Virtual Labs
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:
SMOKING A HOOKAH. THE CATERPILLAR QUESTIONS ALICE AND SHE ADMITS TO HER CURRENT IDENTITY CRISIS, COMPOUNDED BY HER INABILITY TO REMEMBER A POEM. BEFORE CRAWLING AWAY, THE CATERPILLAR TELLS ALICE THAT ONE SIDE OF THE MUSHROOM WILL MAKE HER TALLER AND THE OTHER SIDE WILL MAKE HER SHORTER. SHE BREAKS OFF TWO PIECES FROM THE MUSHROOM. ONE SIDE MAKES HER SHRINK SMALLER THAN EcER, WHILE ANOTHER CAUSES HER NECK TO GROW HIGH INTO THE TREES, WHERE A PIGEON MISTAKES HER FOR A SERPENT. WITH SOME EFFORT, ALICE BRINGS HERSELF BACK TO HER USUAL HEIGHT. SHE STUMBLES UPON A SMALL ESTATE AND USES THE MUSHROOM TO REACH A MORE APPROPRIATE HEIGHT.
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 y by plaintext character q 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:





Conclusion: Thus we learnt and implemented shift cipher and monoalphabetic substitution cipher