

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.



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 EVER, 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 by plaintext character

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

Your replacement history:

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

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 by plaintext character 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 a by A You replaced i by N You replaced x by E You replaced z by I You replaced j by O You replaced e by S You replaced p by T You replaced b by R You replaced a by A You replaced w by L You replaced b by I You replaced i by C You replaced x by E You replaced l by O You replaced d by M You replaced z by S You replaced f by N You replaced u by D You replaced j by T You replaced m by G You replaced k by U You replaced e by H You replaced p by R You replaced o by P You replaced h by W You replaced r by B You replaced t by Y You replaced n by F You replaced g by K You replaced y by Q

Virtual Labs
Virtual Labs
cse29-iiith.vlabs.ac.in/exp/shift-cipher/simulation.html
Gmail YouTube Maps

Virtual Labs
Breaking the Shift Cipher

PART II

Do your rough work here:

PART III

Plaintext:

the porcupine is under the sheets

shift: 3

Ciphertext

ukh arufxslah lv xaghu xkh vkthhev

PART IV

Enter your solution Plaintext and shift key here:

the porcupine is under the sheets

Key: 3

CORRECT!!

Activate Windows

Go to Settings to activate Windows.

Search the web and Windows

2:35 AM 7/20/2022

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