Experiment 01

Breaking the Mono-alphabetic Substitution Cipher using Frequency analysis method.

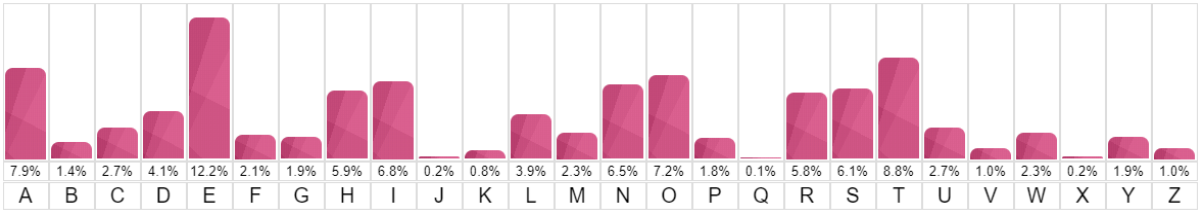
Roll No.	70
Name	Ishika Sanjay Devare
Class	D15-A
Subject	Internet Security Lab
LO Mapped	LO1: To apply the knowledge of symmetric cryptography to implement classical ciphers.

Aim: To understand the process of Breaking the Mono-alphabetic Substitution Cipher using Frequency analysis method.

Introduction:

In cryptography, frequency analysis is the study of the frequency of letters or groups of letters in a ciphertext. The method is used as an aid to breaking substitution ciphers.
Frequency analysis consists of counting the occurrence of each letter in a text. Frequency analysis is based on the fact that, in any given piece of text, certain letters and combinations of letters occur with varying frequencies. For instance, given a section of English language, letters E, T, A and O are the most common, while letters Z, Q and X are not as frequently used.

The following chart shows the frequency of each letter of the alphabet for the English language:



We can assume that most samples of text written in English would have a similar distribution of letters. However, this is only true if the sample of text is long enough. A very short text may lead to a significantly different distribution.

When trying to decrypt a cipher text based on a substitution cipher, we can use a frequency analysis to help identify the most recurring letters in a cipher text and hence make hypothesis of what these letters have been encoded as (e.g., E, T, A, O, etc). This will help us decrypt some of the letters in the text. We can then recognise patterns/words in the partly decoded text to identify more substitutions.

What is Ciphertext?

Ciphertext is encrypted text transformed from plaintext using an encryption algorithm. Ciphertext can't be read until it has been converted into plaintext (decrypted) with a key.

Types of Ciphers-

There are various types of ciphers, including:

1) Substitution ciphers- Replace bits, characters, or character blocks in plaintext with alternate bits, characters or character blocks to produce ciphertext.
   A substitution cipher may be monoalphabetic or polyalphabetic:
   Single alphabet is used to encrypt the entire plaintext message. For example, if the letter A is enciphered as the letter K, this will be the same for the entire message.

   A more complex substitution using a mixed alphabet to encrypt each bit, character or character block of a plaintext message. For instance, the letter A may be encoded as the letter K for part of the message, but later it might be encoded as the letter W.

2) Transposition ciphers. Unlike substitution ciphers that replace letters with other letters, transposition ciphers keep the letters the same, but rearrange their order according to a specific algorithm. For instance, in a simple columnar transposition cipher, a message might be read horizontally but would be written vertically to produce the ciphertext.

3) Polygraphic ciphers- Substituting one letter for another letter, a polygraphic cipher performs substitutions with two or more groups of letters. This masks the frequency distribution of letters, making frequency analysis attacks much more difficult.

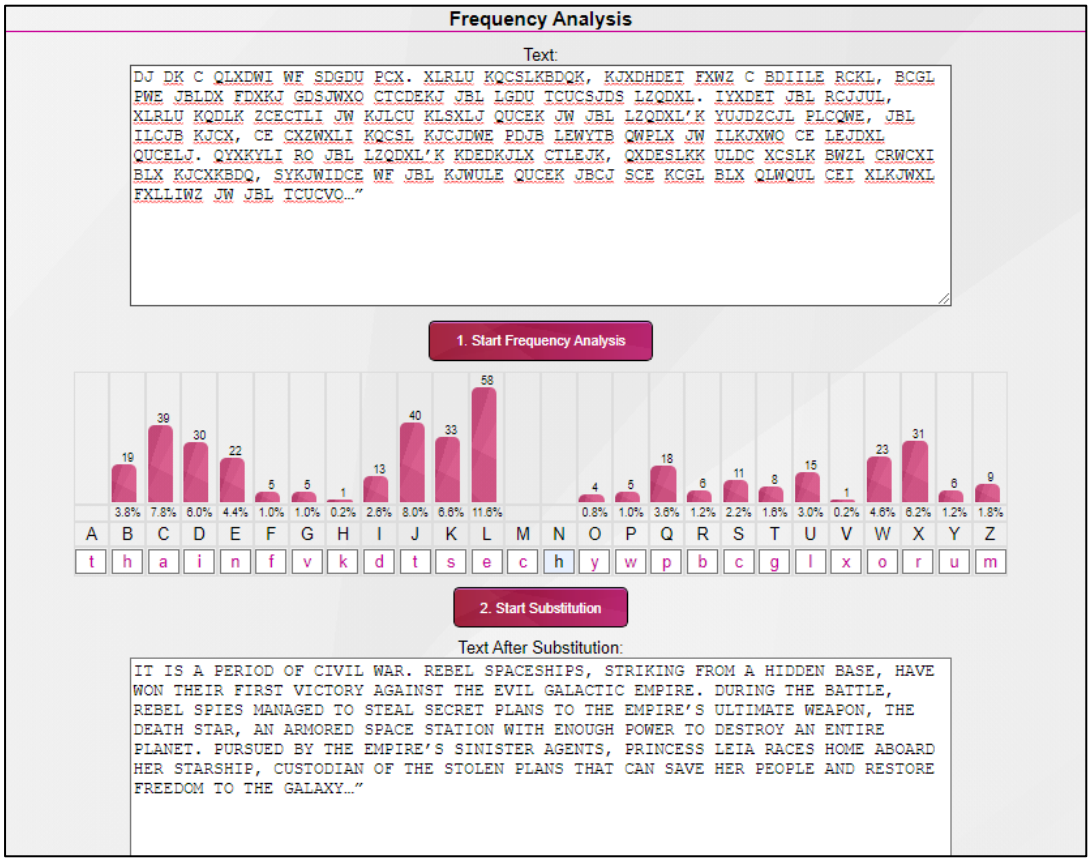
4) Permutation ciphers- In this cipher, the positions held by plaintext are shifted to a regular system so that the ciphertext constitutes a permutation of the plaintext.

5) Private-key cryptography- In this cipher, the sender and receiver must have a pre-shared key. The shared key is kept secret from all other parties and is used for encryption, as well as decryption.

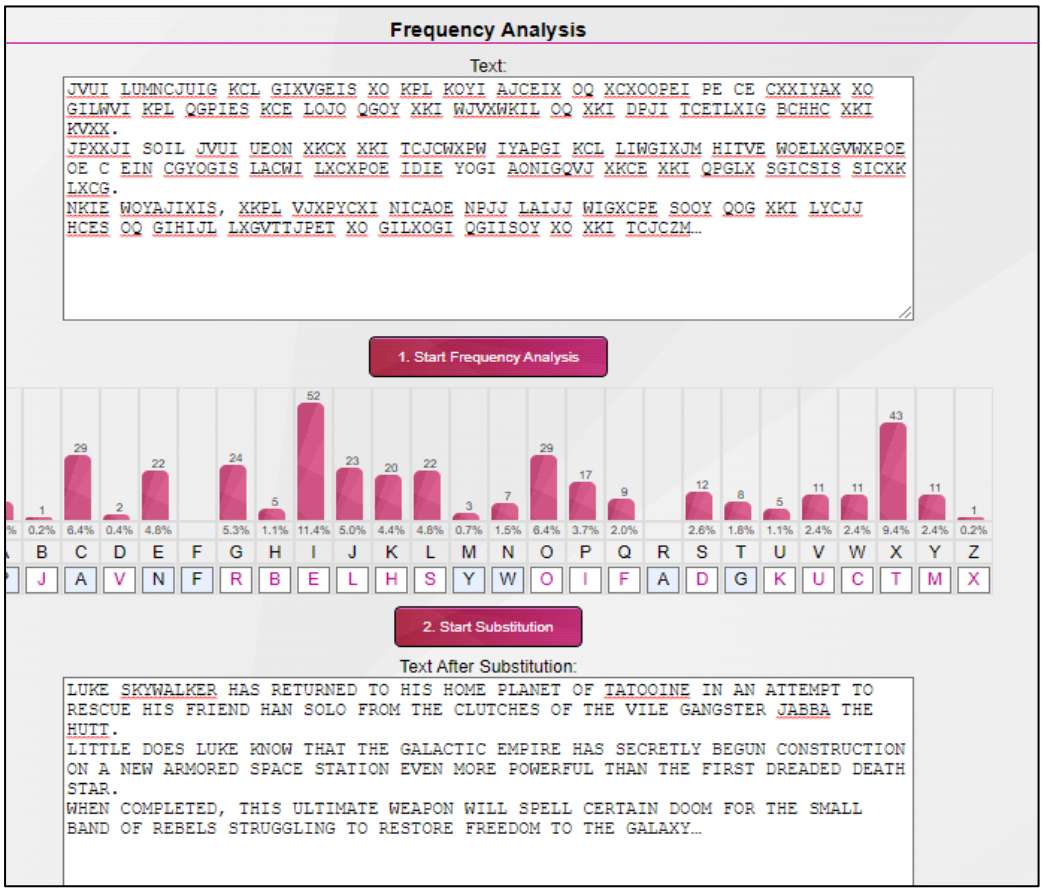
6) Public-key cryptography- In this cipher, two different keys -- public key and private key -- are used for encryption and decryption. The sender uses the public key to perform the encryption, but the private key is kept secret from the receiver.

Results:

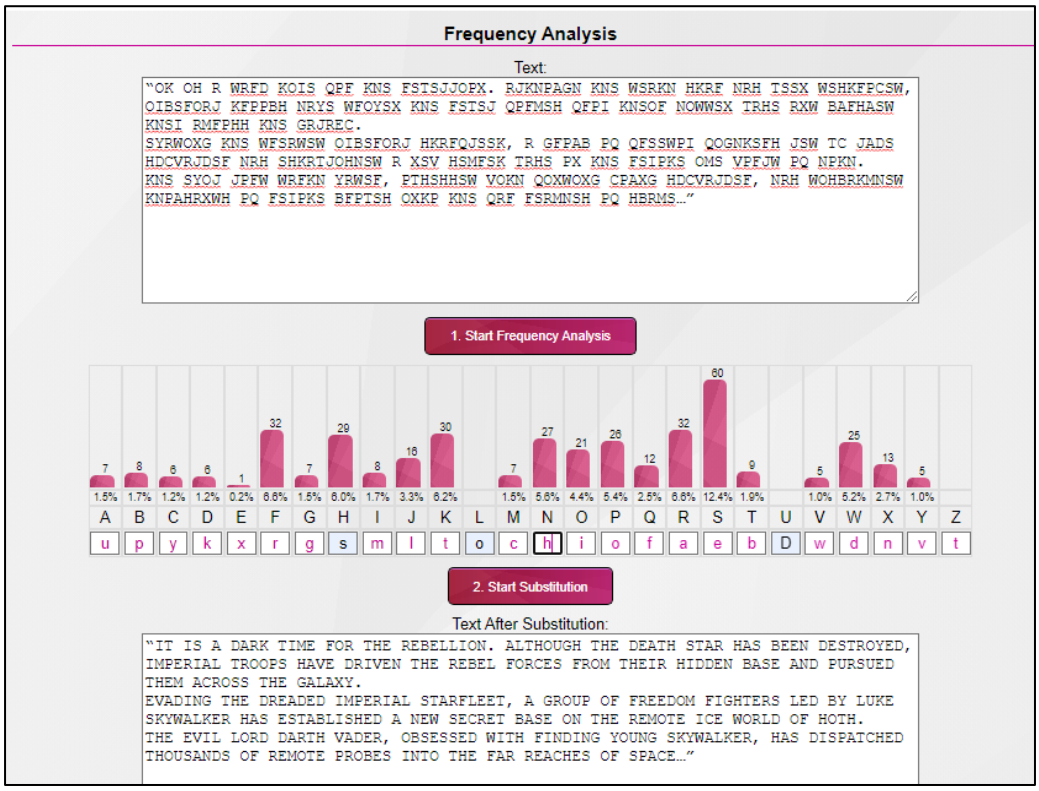
Cipher 1:



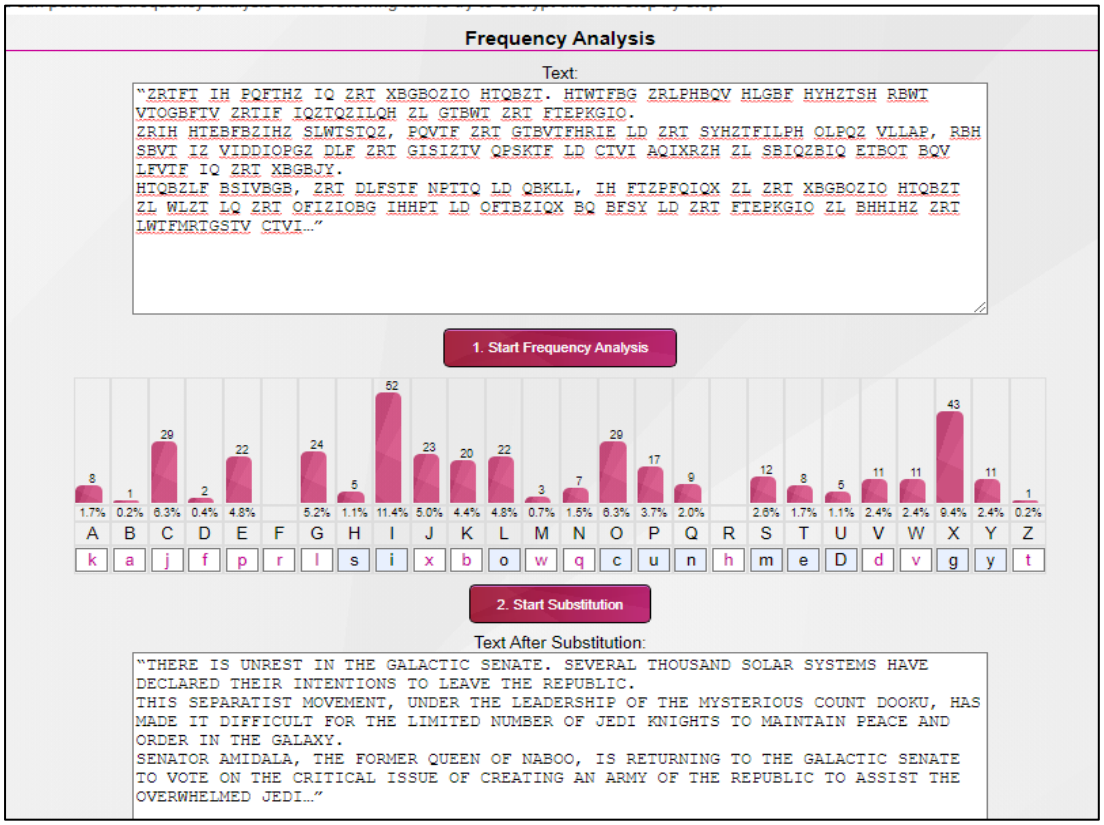
Cipher 2:



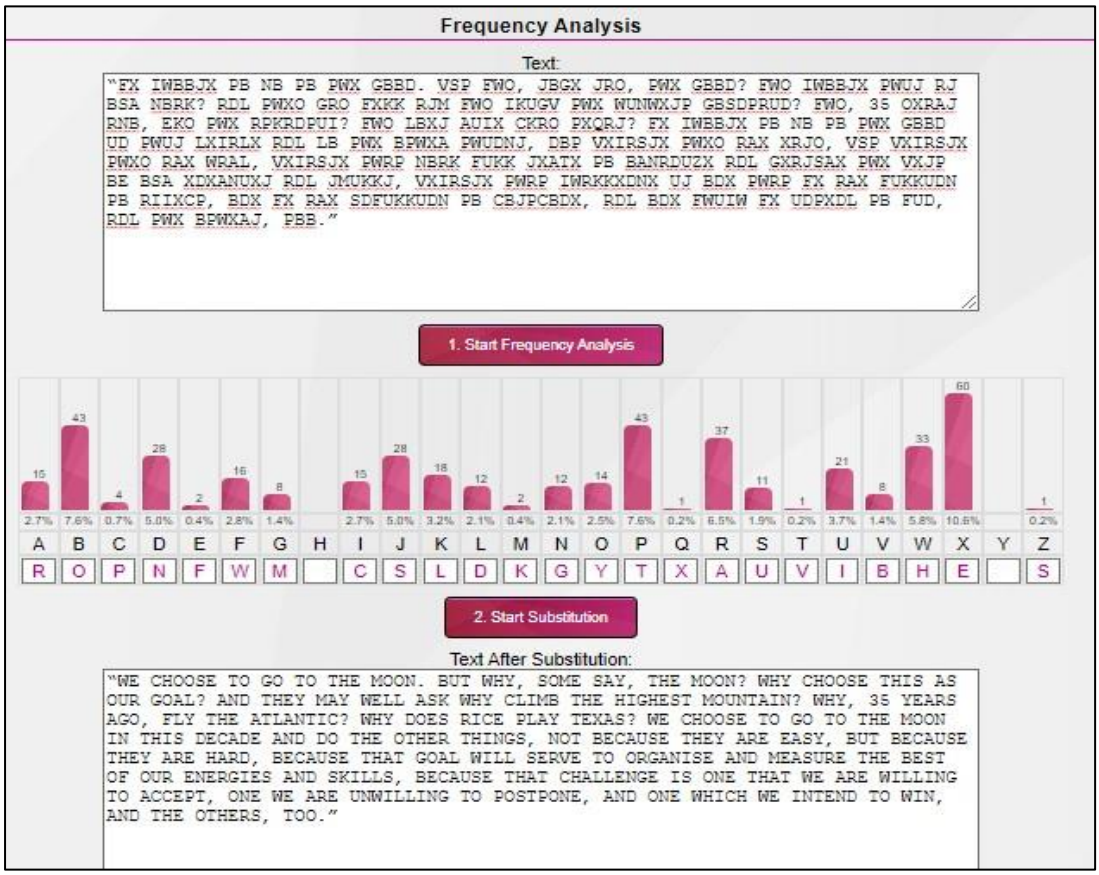
Cipher 3:



Cipher 4:



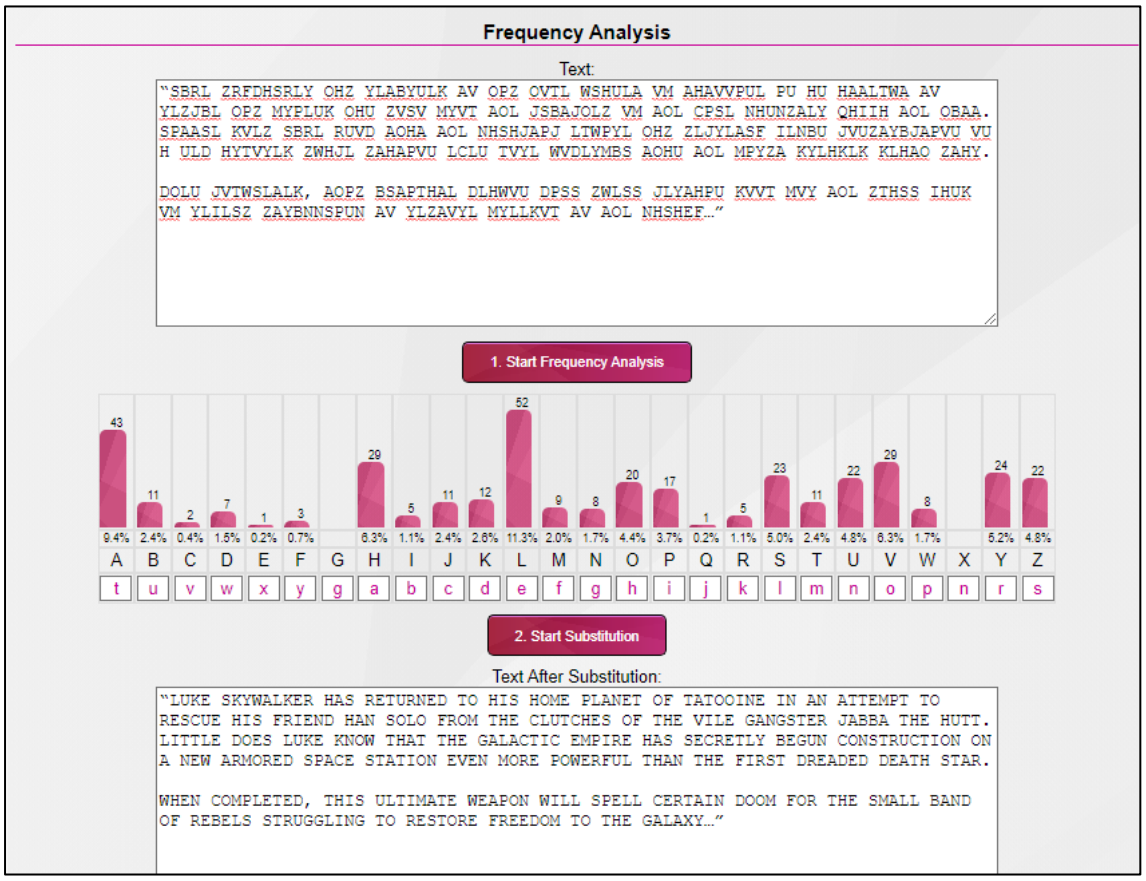
Cipher 5:



Cipher 6:

Cipher 7:

Cipher 8:



Conclusion: We successfully understood the process of Breaking the Mono-alphabetic Substitution Cipher using Frequency analysis method.