Experiment 01

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

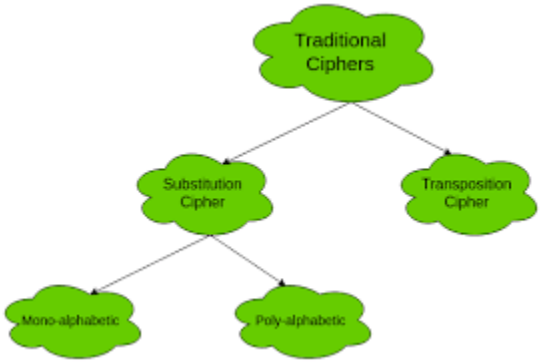
Roll No.	17
Name	Manav Jawrani
Class	D15-A
Subject	Internet Security Lab
LO Mapped	LO1: To apply the knowledge of symmetric cryptography to implement classical ciphers.

Aim: Write a program to understand Breaking the Mono-alphabetic Substitution Cipher using Frequency analysis method.

Introduction:

What is a Substitution Cipher?

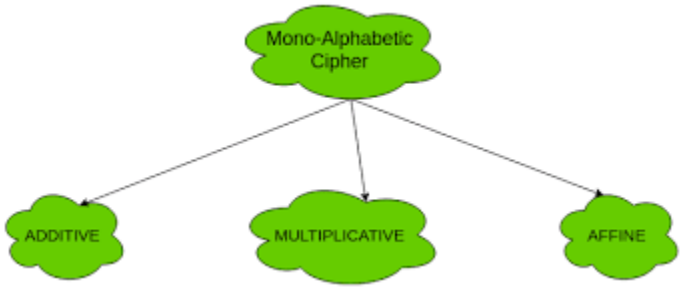
- In cryptography, a **substitution cipher** is a method of encrypting in which units of plaintext are replaced with the ciphertext, in a defined manner, with the help of a key; the "units" may be single letters (the most common), pairs of letters, triplets of letters, mixtures of the above, and so forth. The receiver deciphers the text by performing the inverse substitution process to extract the original message.Substitution ciphers can be compared with transposition ciphers. In a transposition cipher, the units of the plaintext are rearranged in a different and usually quite complex order, but the units themselves are left unchanged. By contrast, in a substitution cipher, the units of the plaintext are retained in the same sequence in the ciphertext, but the units themselves are altered.
- Types of substitution cipher are:
    1. Monoalphabetic Substitution Cipher
    2. Polyalphabetic Substitution Cipher



What is a Mono-alphabetic Substitution Cipher?

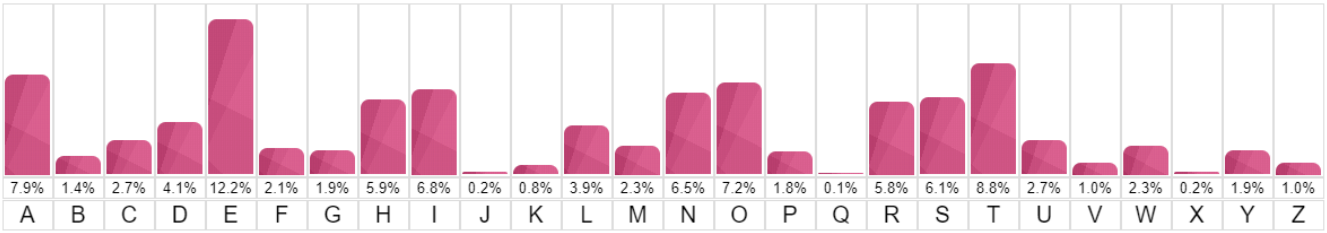
- Monoalphabetic cipher is a substitution cipher in which for a given key, the cipher alphabet for each plain alphabet is fixed throughout the encryption process. For example, if ‘A’ is encrypted as ‘D’, for any number of occurrences in that plaintext, ‘A’ will always get encrypted to ‘D’.
- There are various techniques of Monoalphabetic cipher which are as follows

1. Additive Cipher − Additive cipher is one method of changing a permutation of the letters of the alphabet. Each letter in the alphabet is cyclically changed by the equivalent amount and the relative order of the letters is kept similar
2. Multiplicative Cipher − Multiplicative cipher is another method for creating a permutation of the letters of the alphabet. It can take a key value and each letter's position number is multiplied by 5 and thus the product is decreased by modulo 26.
3. Affine Cipher − The Affine cipher is a type of monoalphabetic substitution cipher, wherein each letter in an alphabet is mapped to its mathematical equivalent, encrypted using a simple mathematical function, and transformed back to a letter.



What is frequency analysis in cryptography?

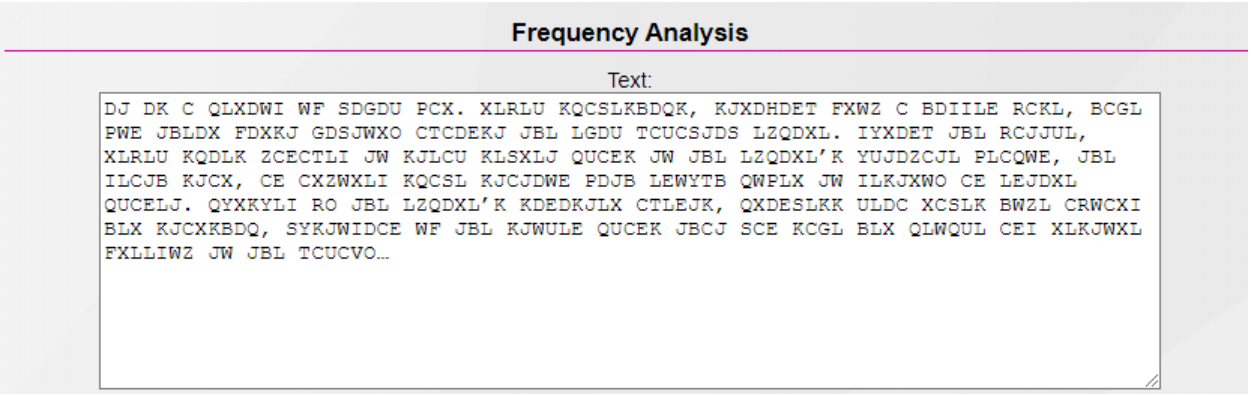
- In cryptography, frequency analysis is the study of the frequency of letters or groups of letters in a ciphertext. The method is used as an aid to breaking substitution ciphers for e.g. mono-alphabetic substitution cipher. Frequency analysis consists of counting the occurrence of each letter in a text. 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.



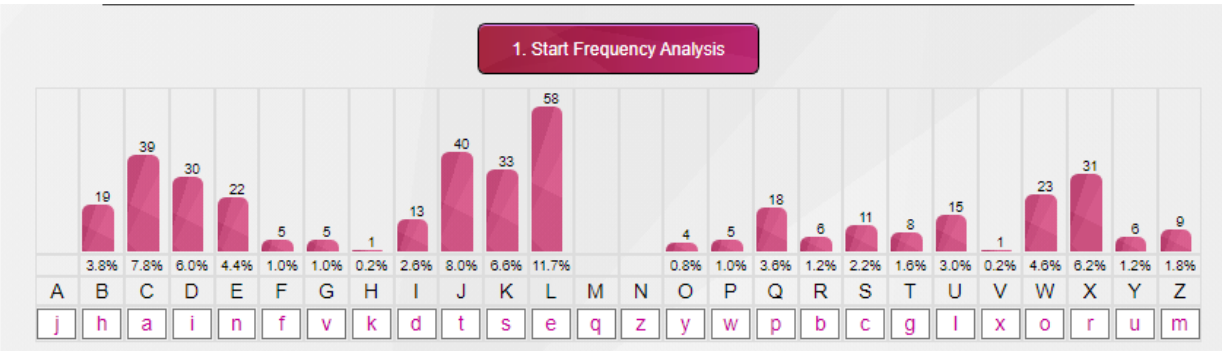
Results:

1. Problem 1

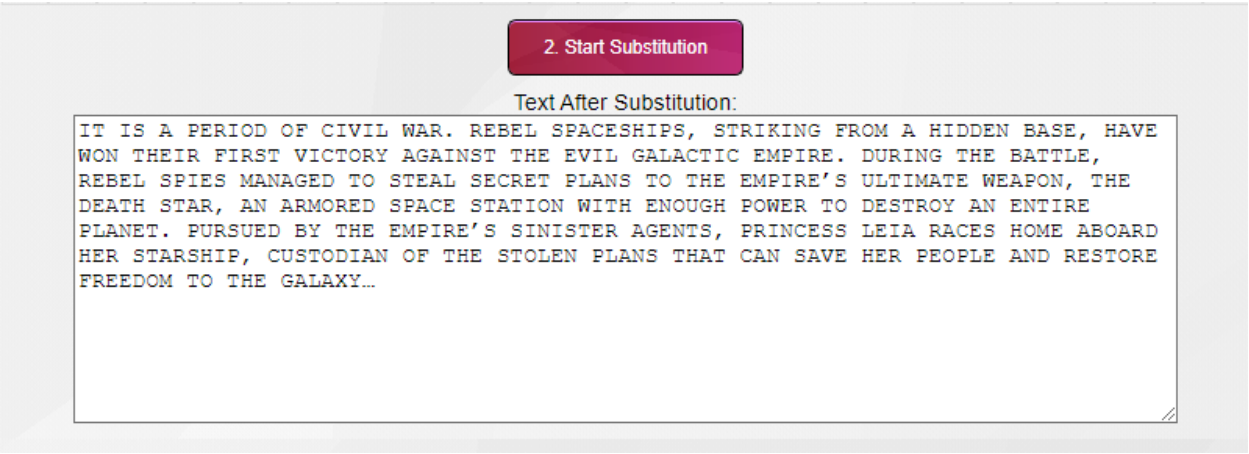
Cipher Text:



Frequency Analysis:



Plain Text:

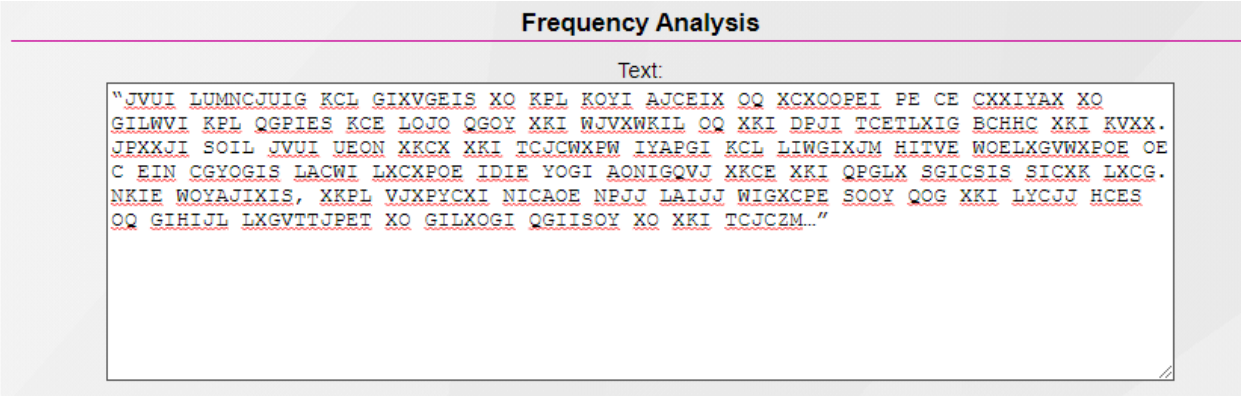


Observations:

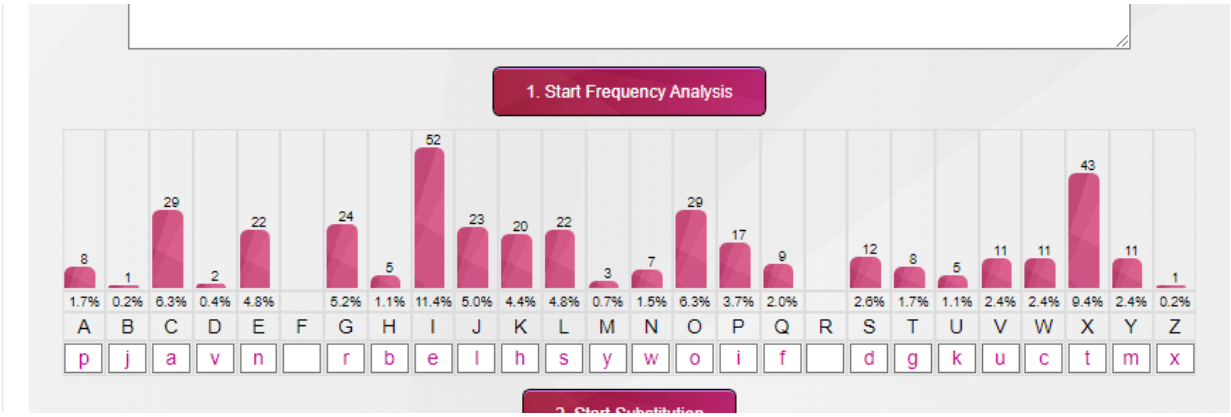
In this problem we have observed that there is a random mono-alphabetic substitution where the letters A,M,N are not used to hide other letters and letter L is used the most.

2. Problem 2

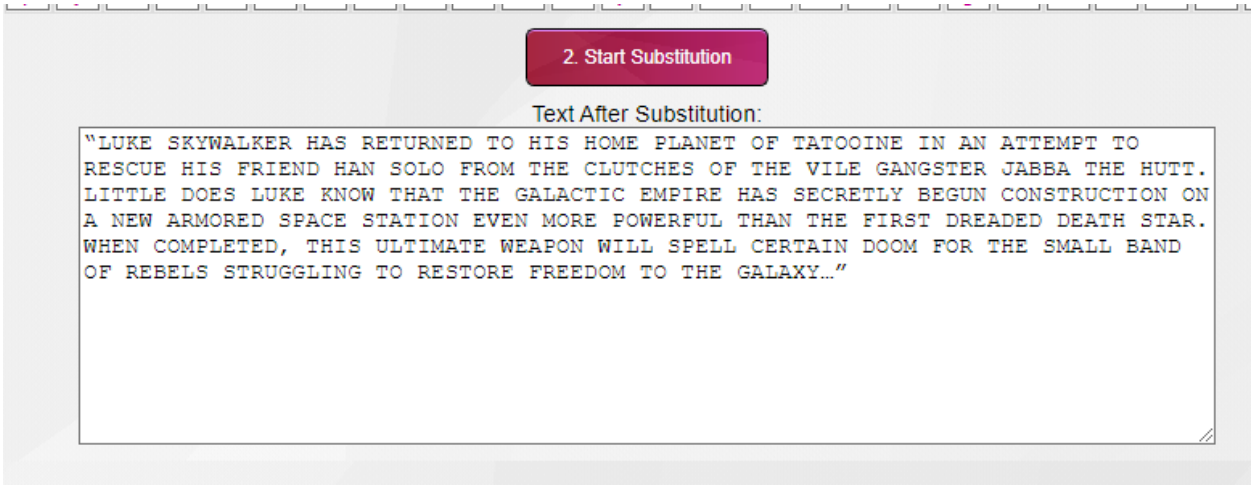
Cipher Text:



Frequency Analysis:



Plain Text:

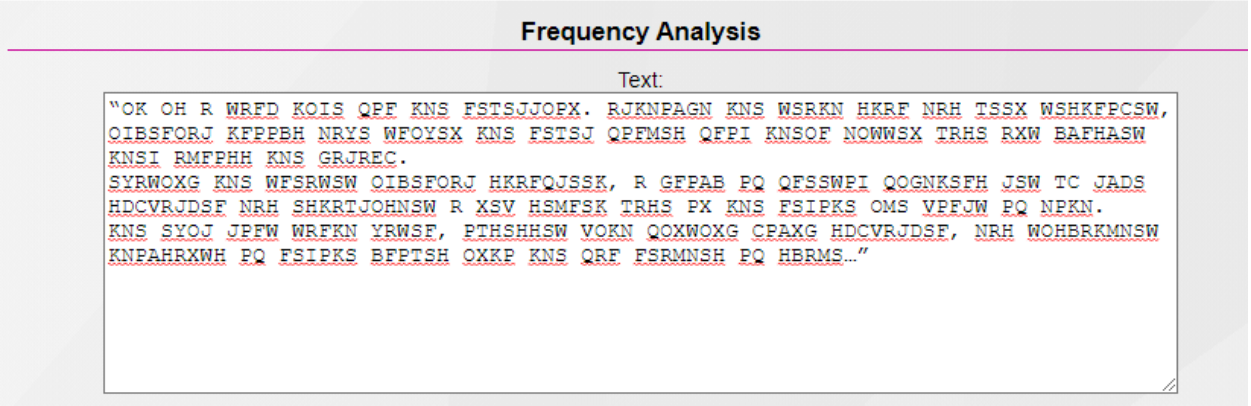


Observations:

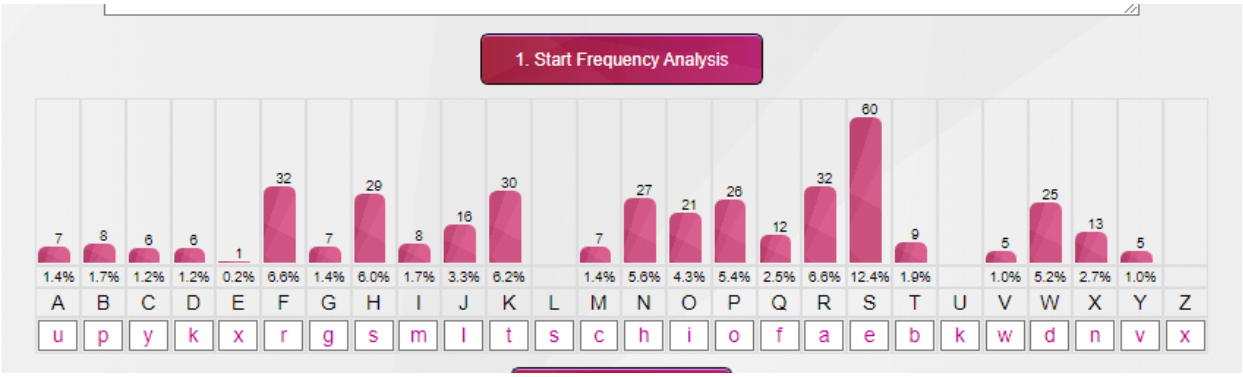
In this problem we have observed that there is a random mono-alphabetic substitution where the letters F,R are not used to hide other letters and letter I is used the most.

3. Problem 3

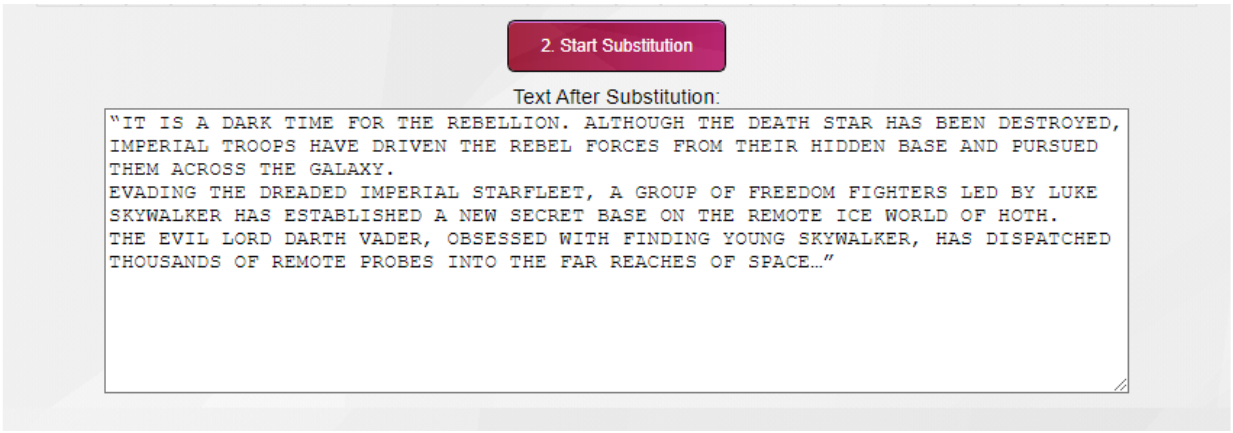
Cipher Text:



Frequency Analysis:



Plain Text:

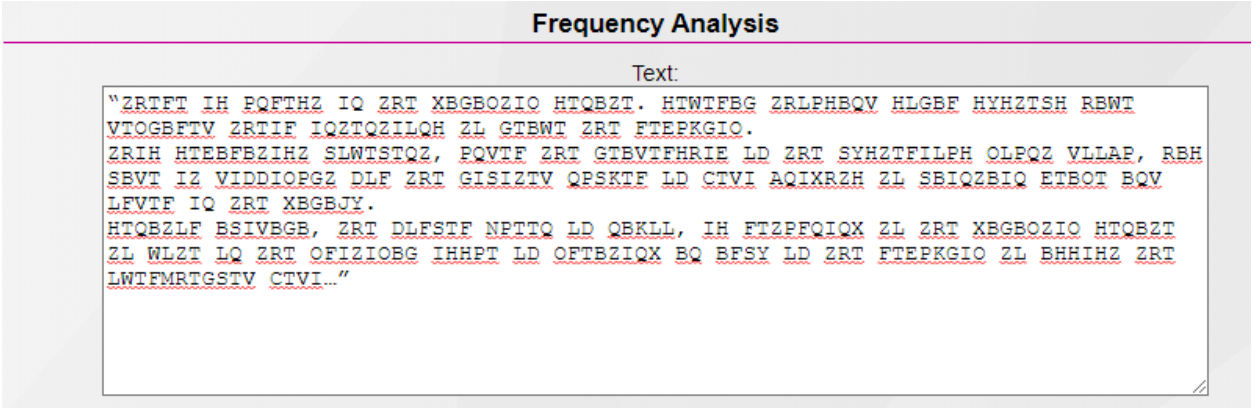


Observations:

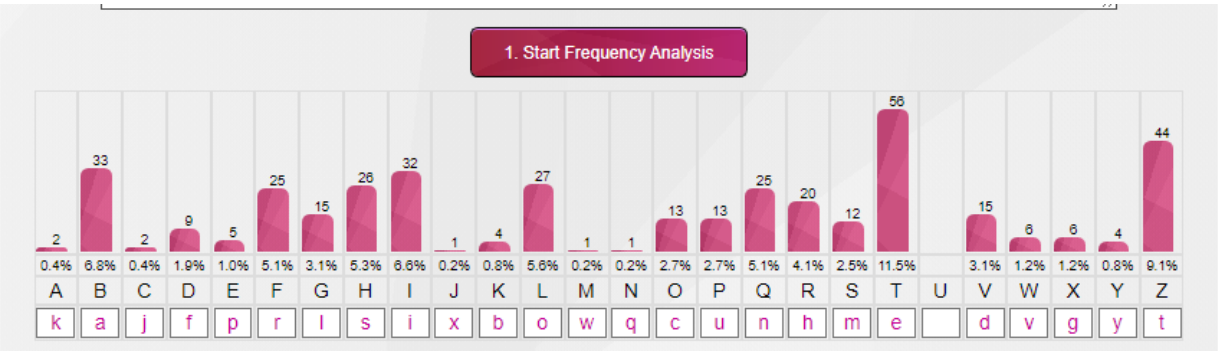
In this problem we have observed that there is a random mono-alphabetic substitution where letters L,U are not used to hide other letters and letter S is used the most.

4. Problem 4

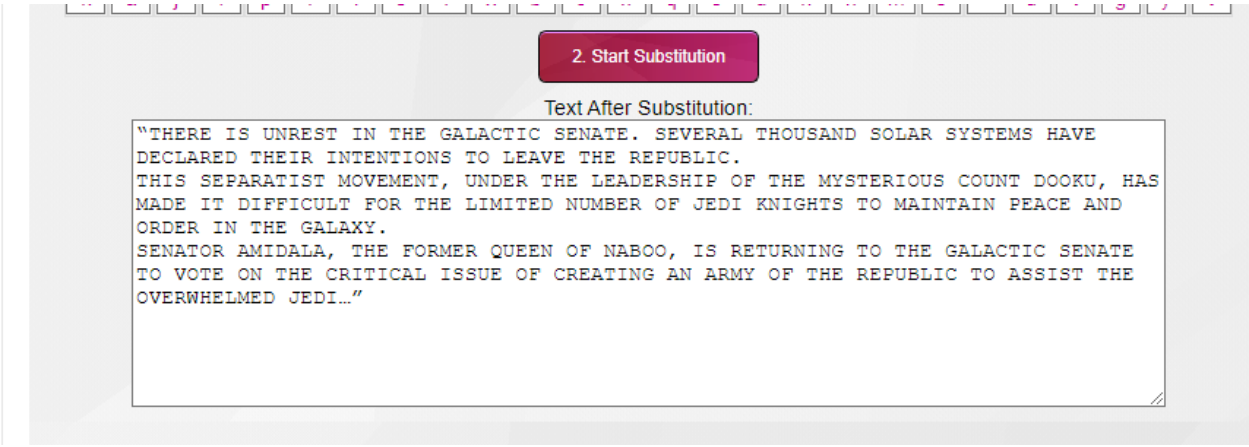
Cipher Text:



Frequency Analysis:



Plain Text:

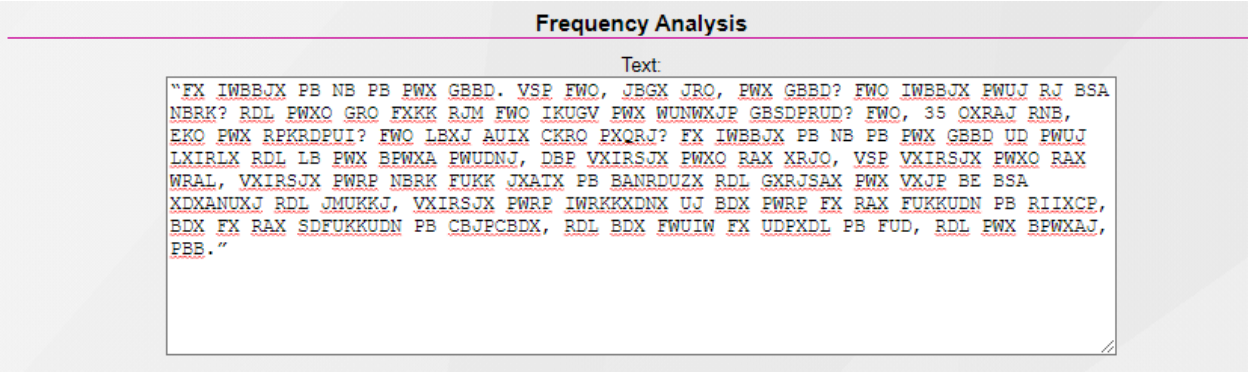


Observations:

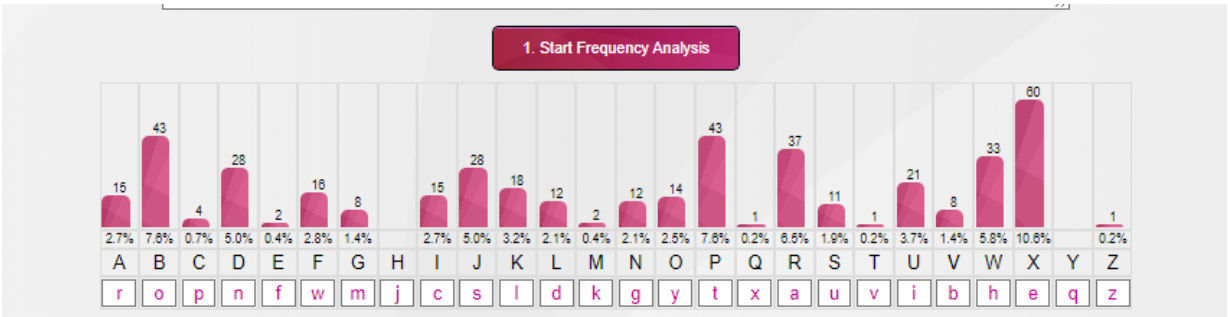
In this problem we have observed that there is a random mono-alphabetic substitution where letter U is not used to hide other letters and letter T is used the most.

5. Problem 5

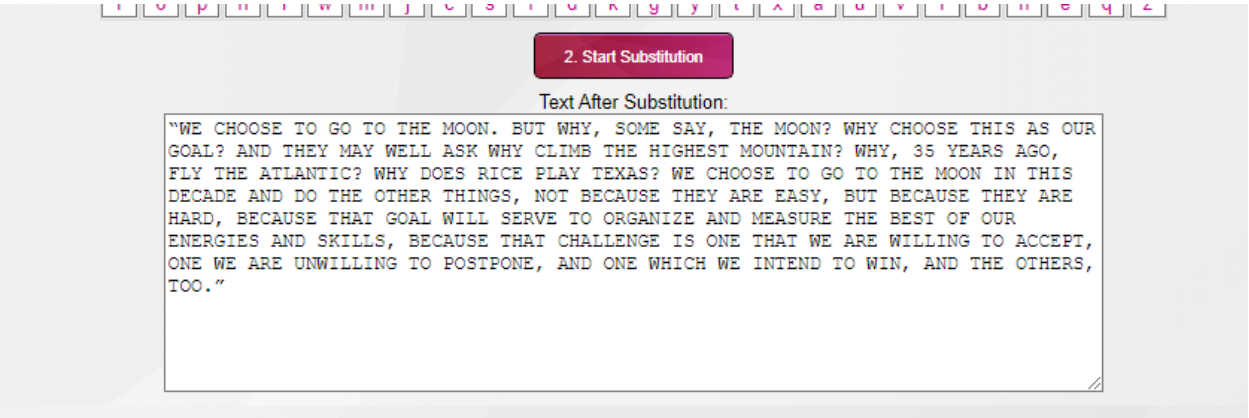
Cipher Text:



Frequency Analysis:



Plain Text:

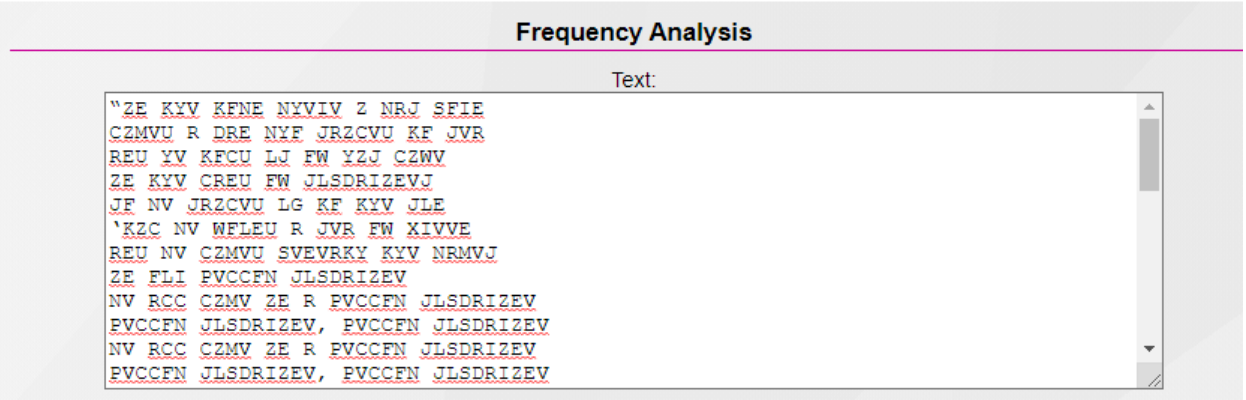


Observations:

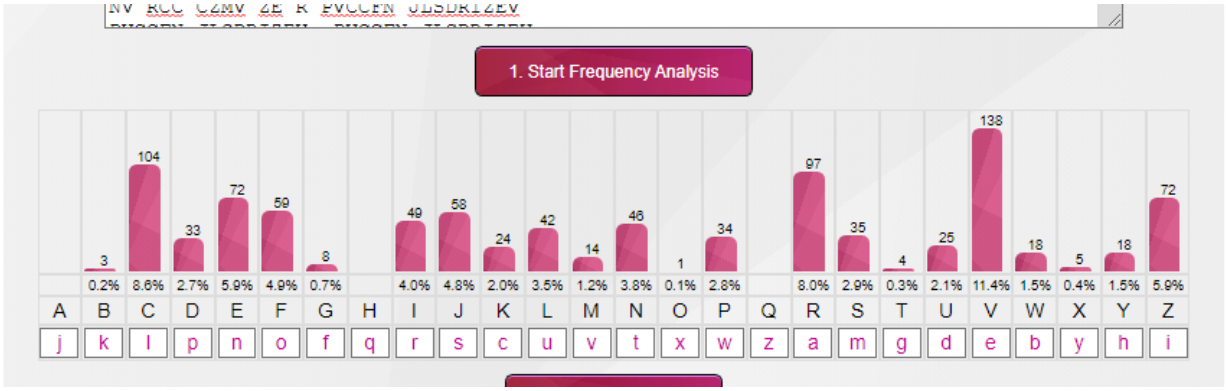
In this problem we have observed that there is a random mono-alphabetic substitution where letters H,Y is not used to hide other letters and letter X is used the most.

6. Problem 6

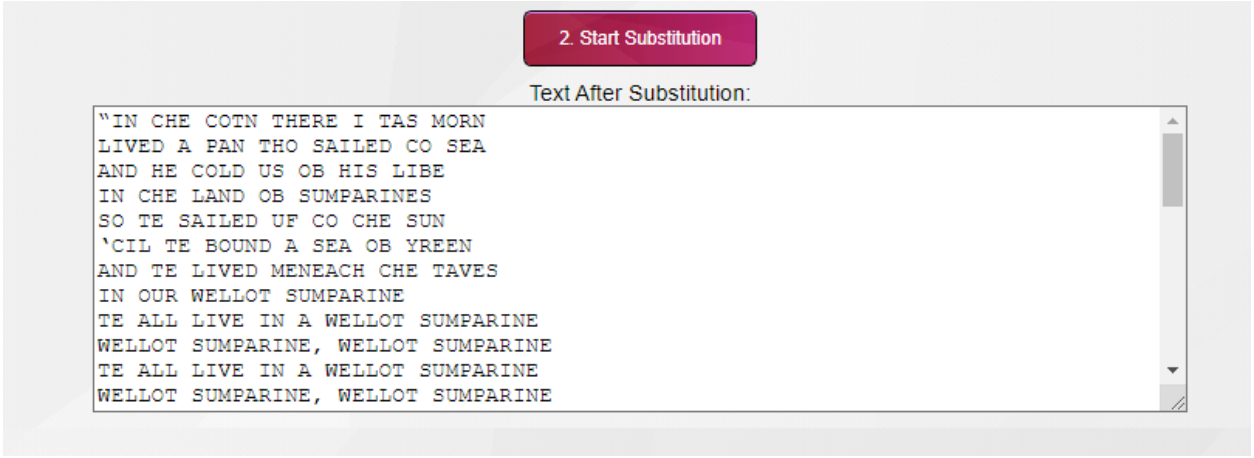
Cipher Text:



Frequency Analysis:



Plain Text:

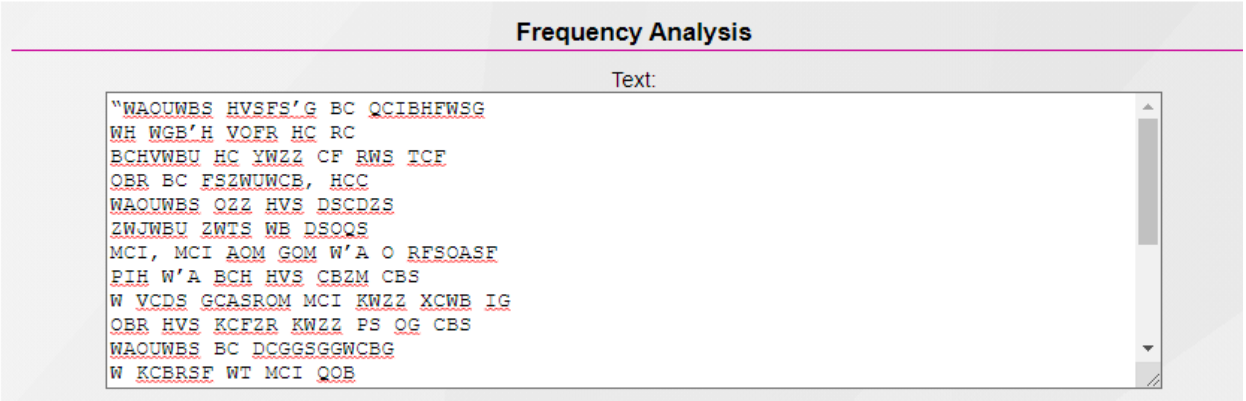


Observations:

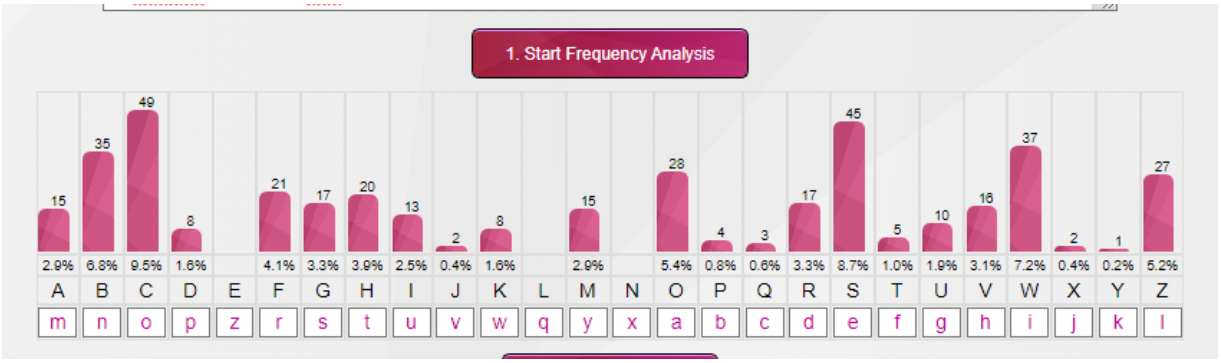
In this problem we have observed that there is a random mono-alphabetic substitution where letters A,H,Q are not used to hide other letters and letter V is used the most.

7. Problem 7

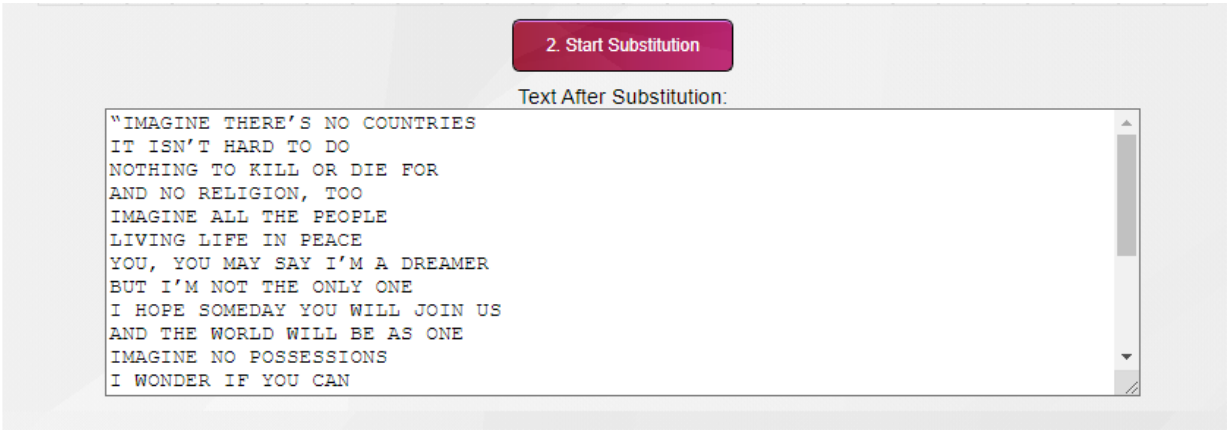
Cipher Text:



Frequency Analysis:



Plain Text:

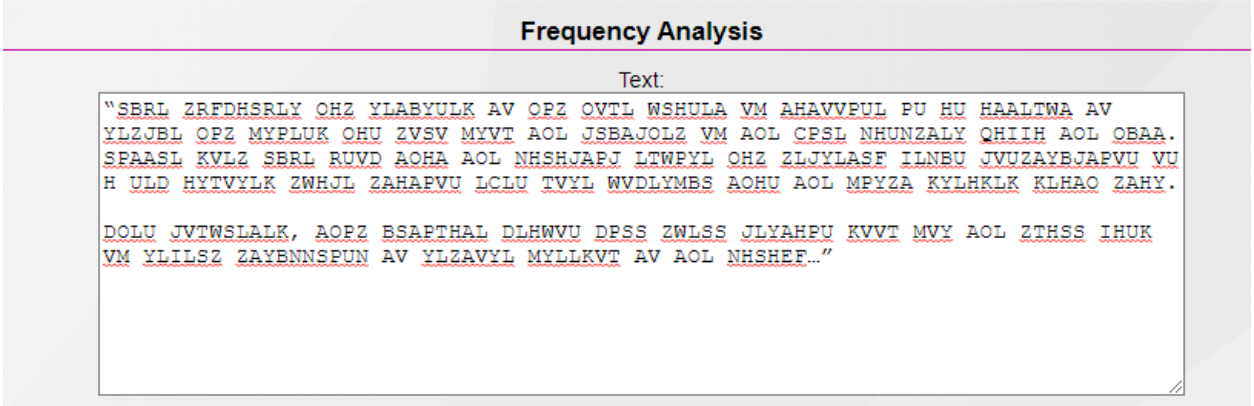


Observations:

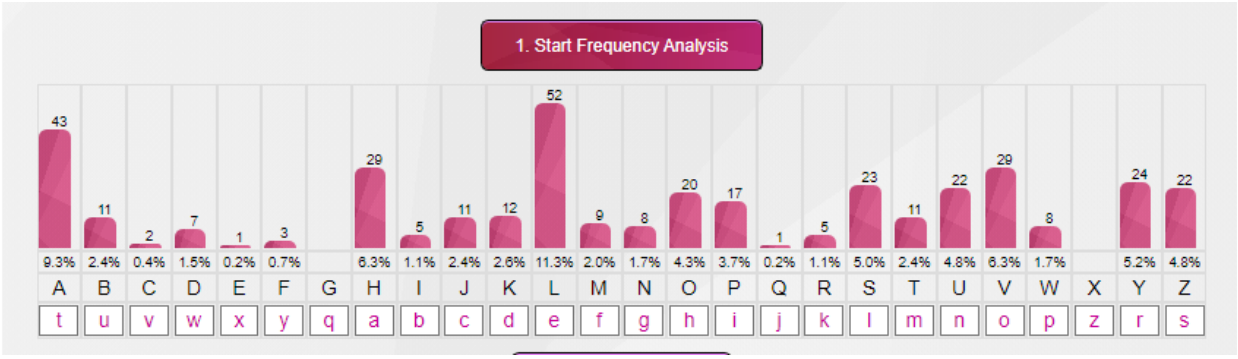
In this problem we have observed that there is a random mono-alphabetic substitution where letters E,L,N are not used to hide other letters and letter C is used the most.

8. Problem 8

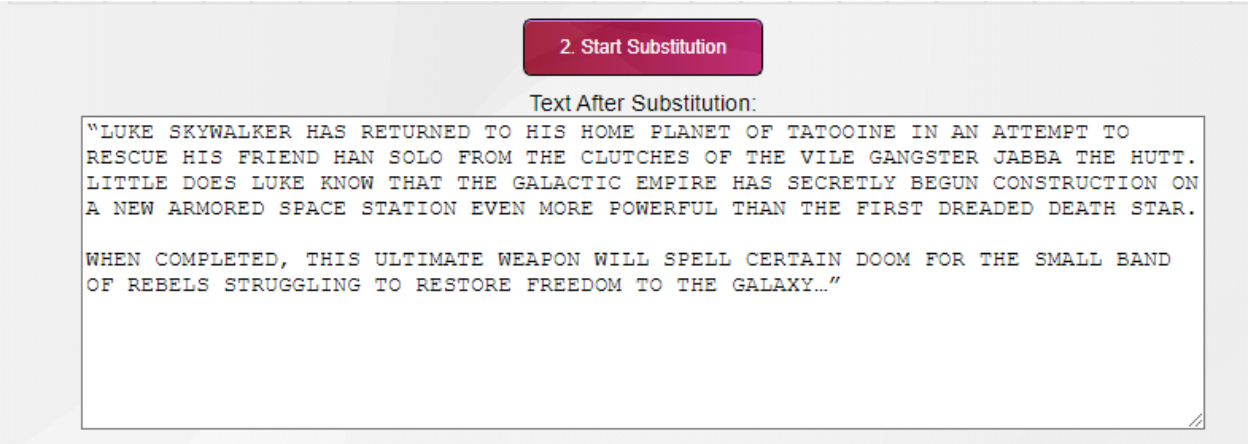
Cipher Text:



Frequency Analysis:



Plain Text:



Observations:

In this problem we have observed that there is a random mono-alphabetic substitution where letters G,X are not used to hide other letters and letter L is used the most.

Conclusion:

We have successfully broken the mono-alphabetic substitution cipher using frequency analysis and understood how the mono-alphabetical substitution cipher works.