Experiment No. 01

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

Theory:

Mono-alphabetic Substitution Cipher:

A mono-alphabetic substitution cipher is a type of substitution cipher where each letter of the plaintext is replaced with a fixed corresponding letter from the cipher alphabet. In other words, it involves mapping each letter of the alphabet to a different letter. The key to the cipher is the mapping between the plaintext alphabet and the cipher alphabet.

For example, using a simple mono-alphabetic substitution cipher with a fixed key, the mapping might look like this:

Plaintext: ABCDEFGHIJKLMNOPQRSTUVWXYZ

Cipher: XYZABCDEFGHIJKLMNOPQRSTUVW

Advantages of Mono-alphabetic Substitution Cipher:

Ease of Implementation: Mono-alphabetic ciphers are relatively easy to implement and understand, making them accessible for educational purposes or simple encryption needs.

Initial Security: Mono-alphabetic ciphers can provide some basic level of security against casual attempts at decryption, especially if the cipher alphabet is randomly generated.

Disadvantages of Mono-alphabetic Substitution Cipher:

Vulnerable to Frequency Analysis: The biggest weakness of mono-alphabetic substitution ciphers is that each letter in the plaintext is always mapped to the same letter in the ciphertext. This leads to patterns in the ciphertext, making it susceptible to frequency analysis.

Limited Key Space: The key space of mono-alphabetic substitution ciphers is relatively small since there are only 26! (factorial) possible key combinations. This makes brute-force attacks feasible, especially with the aid of frequency analysis.

Lack of Perfect Secrecy: Unlike more complex ciphers like the one-time pad, mono-alphabetic substitution ciphers do not provide perfect secrecy. Once the key is discovered, the entire message can be decrypted.

Frequency Analysis Method:

Frequency analysis is a technique used to break mono-alphabetic substitution ciphers or ciphers with relatively weak encryption methods. It takes advantage of the fact that certain letters or combinations of letters occur with predictable frequency in natural languages like English.

The steps in a frequency analysis attack are as follows:

Collect Ciphertext: Obtain the encrypted message that you want to decrypt.

Analyze Frequency: Count the occurrences of each letter in the ciphertext. Certain letters will have higher frequencies due to their prevalence in the language.

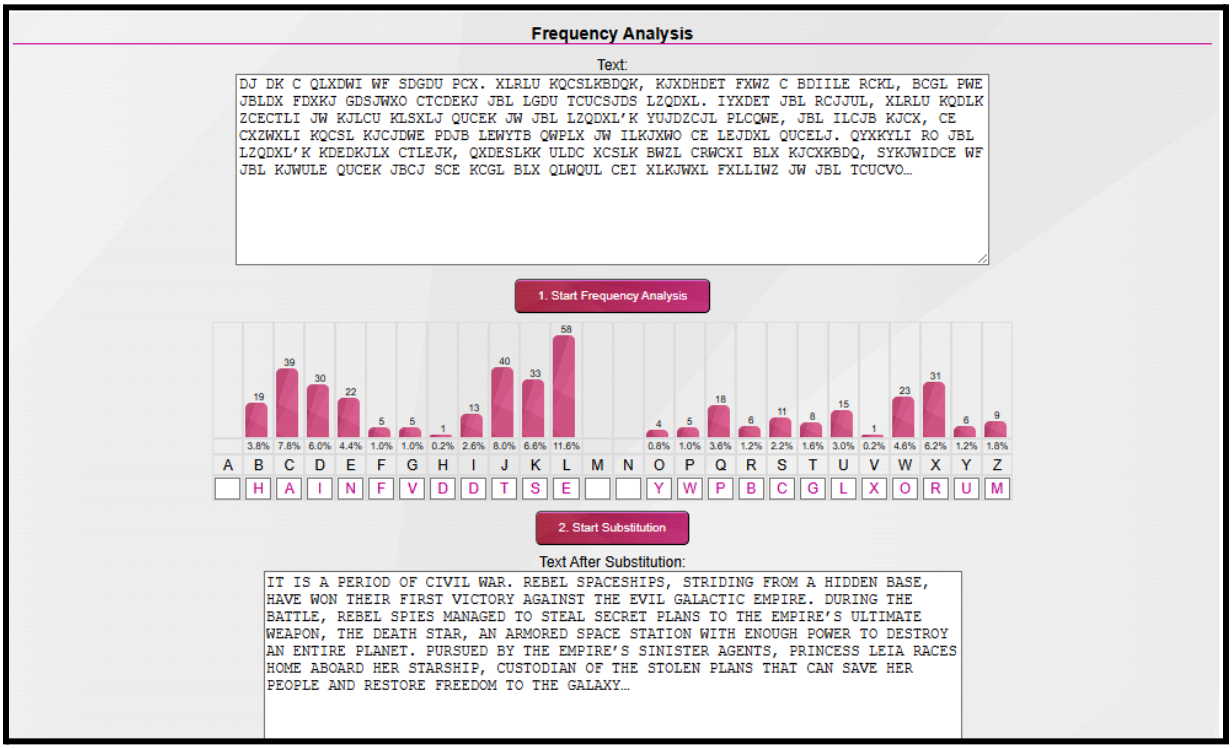
Map Frequencies: Map the most frequently occurring letters in the ciphertext to the most frequently occurring letters in the language (e.g., 'E' in English).

Compare Context: Use the context of the message to identify other words and patterns to gradually piece together the key and the original plaintext.

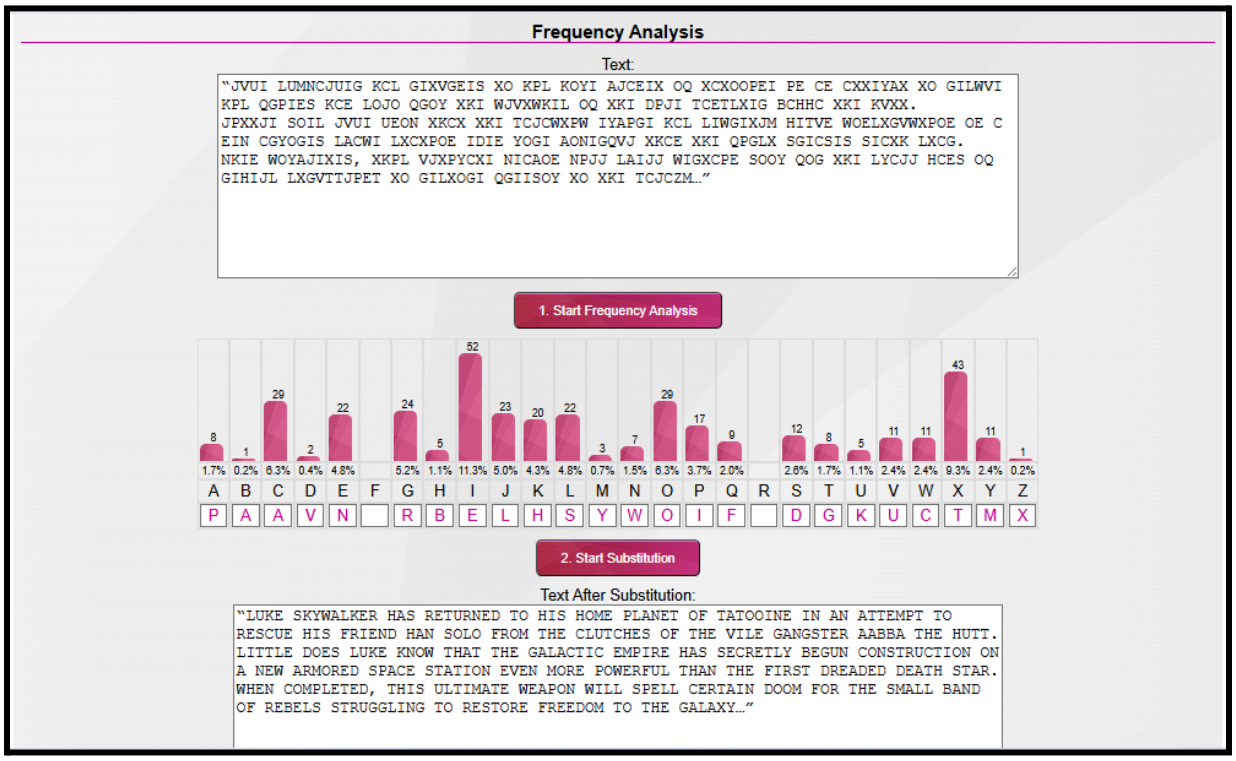
Trial and Error: In more complex cases, frequency analysis may not fully decrypt the entire message, but it can significantly reduce the key space, allowing for manual trial and error to find the correct decryption.

Frequency analysis is particularly effective against longer ciphertexts because it provides more data for analyzing letter frequencies. To counter frequency analysis, more secure ciphers, such as poly-alphabetic ciphers or modern cryptographic algorithms like AES, were developed, which are not vulnerable to this type of attack.

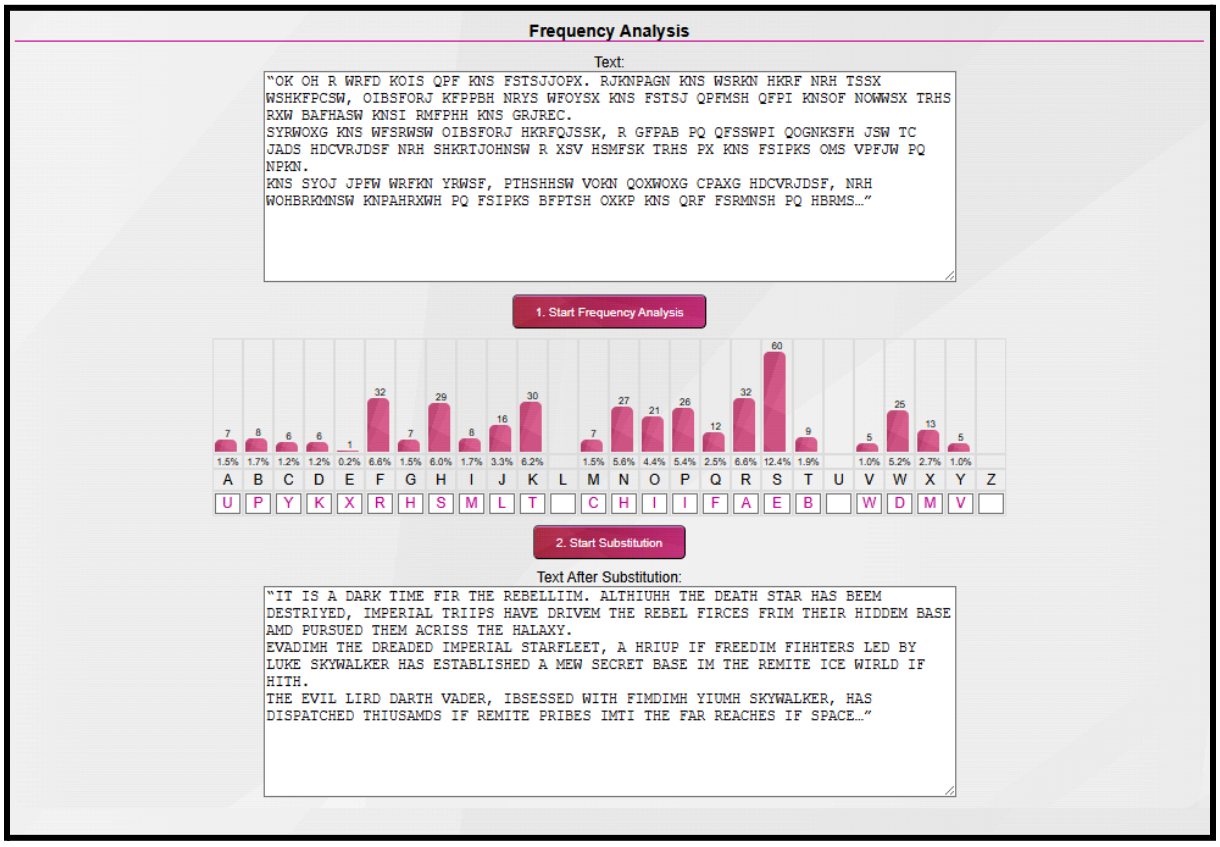
Cipher 1:



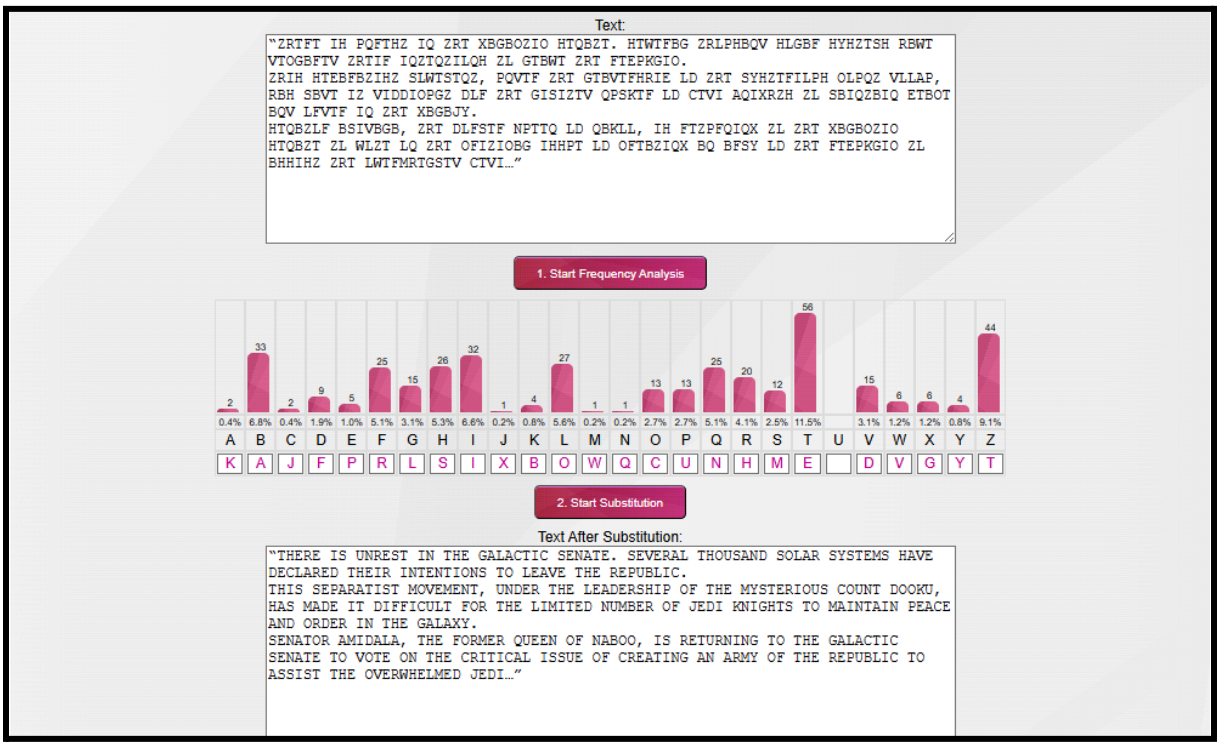
Cipher 2



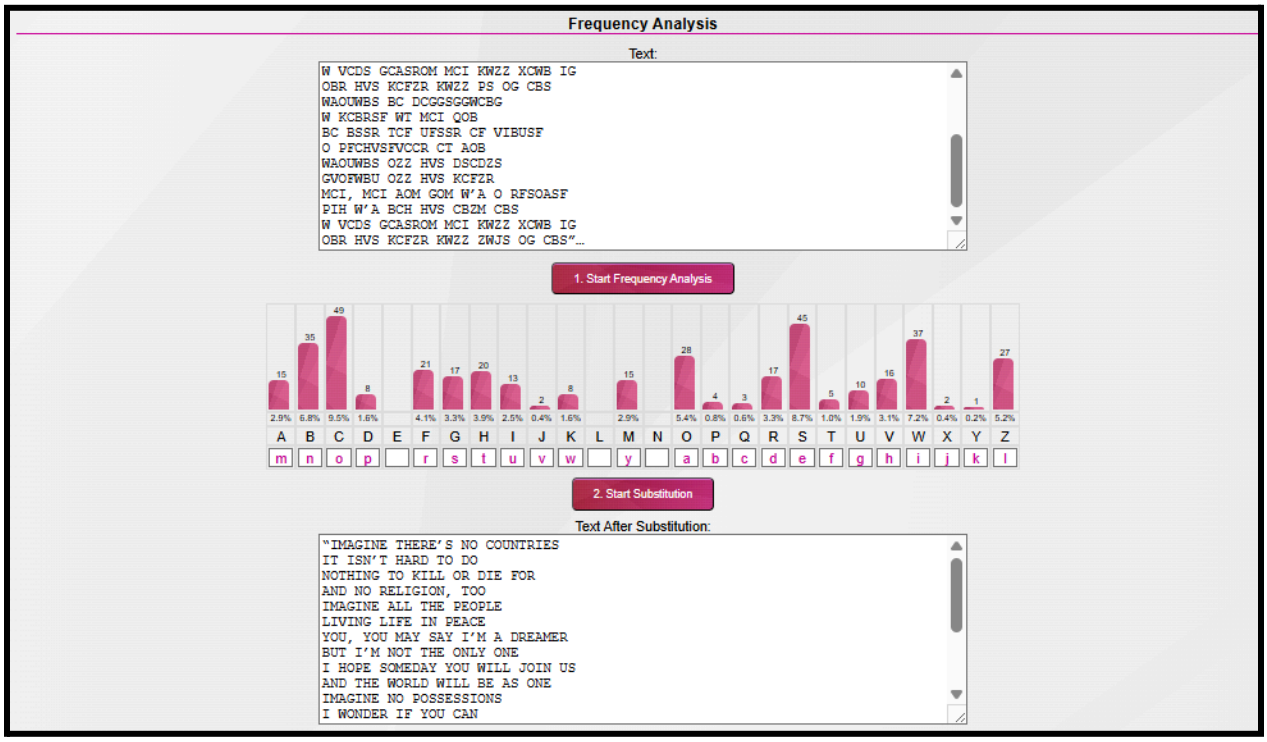
Cipher 3:



Cipher 4:



Cipher 5



Answer in brief for the below questions:

1. What is the primary weakness of monoalphabetic cipher?

A. The **primary weakness of a monoalphabetic cipher** lies in its vulnerability to **frequency analysis**. Since each plaintext letter is always replaced by the same ciphertext letter, the statistical patterns of the language remain preserved. For example, in English, the letter **E** is the most common, followed by **T, A, O, I, N**. An attacker can study the frequency of letters in the ciphertext and match them with these common frequencies. Once a few substitutions are guessed, the rest of the message can usually be reconstructed easily.

2. How can you decode a message encrypted with a monoalphabetic cipher without knowing the key?

A. A **message encrypted with a monoalphabetic cipher can be decoded without knowing the key** by using cryptanalysis. The most common method is **frequency analysis**, where the attacker counts how often each symbol occurs in the ciphertext and

compares it with known letter frequencies in the language. Repeated patterns also help; for example, one-letter words are likely to be **A** or **I**, and common digraphs such as **TH, HE, IN** appear frequently. Once partial substitutions are made, the remaining letters can be revealed through pattern recognition and context-based guessing. Modern tools automate this process, making it even faster.

3. Can a monoalphabetic cipher be used to encode numbers and symbols as well as letters?

A. Monoalphabetic ciphers are not limited to letters; they **can be extended to encode numbers and symbols** as well. This is done by enlarging the substitution alphabet to include digits and punctuation marks. For example, the digit **0** might be substituted by a symbol like #, or a period might be replaced by +. However, this extension does not remove the cipher's weakness because numbers and symbols also follow predictable patterns of use (for instance, years like 2024 contain repeating digits, and punctuation like commas and full stops occur regularly). Thus, frequency analysis can still be applied.

4. What is a substitution table, and how is it used in monoalphabetic ciphers?

A. A **substitution table** is a chart that defines the mapping between plaintext characters and their ciphertext equivalents in a monoalphabetic cipher. It essentially acts as the "key" to the cipher. For encryption, each plaintext letter is replaced by the corresponding ciphertext symbol according to the table. For decryption, the process is reversed. For instance, in a Caesar cipher shifted by three places, **A** is mapped to **D**, **B** to **E**, and so on. Cryptanalysts also build partial substitution tables while breaking a cipher by gradually filling in the guessed mappings. This table form makes both encryption and decryption systematic and easy to follow.