Assignment Number: 1

Name: Divya Shah; Branch: I.T (T.E.); Roll Number: 115 24/08/2023

Aim: Breaking shift cipher and Mono-alphabetic Substitution Cipher using Frequency analysis method.

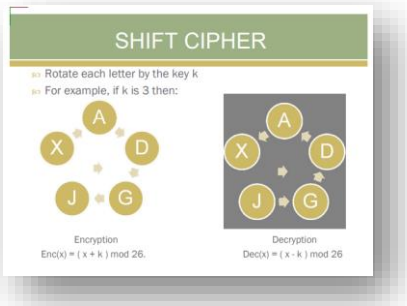
LO mapped: LO1

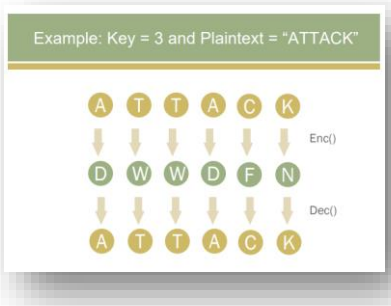
Theory:

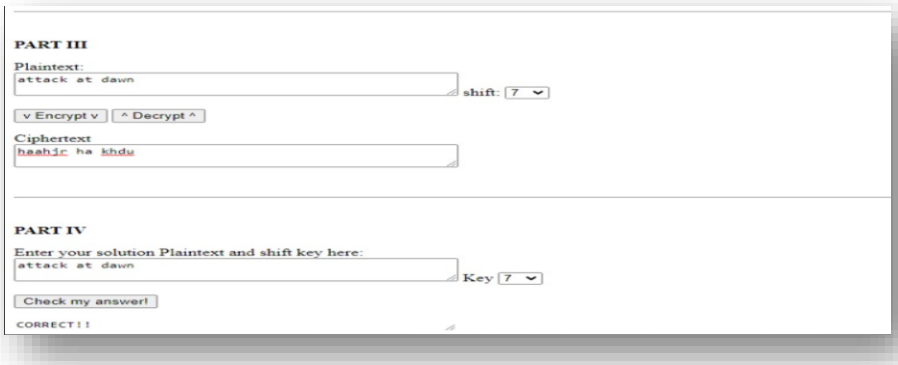
This assignment delves into the fundamental concepts of classical cryptography by exploring two commonly used encryption techniques: the Shift Cipher and the Mono-Alphabetic Substitution Cipher. The primary objective is to understand the vulnerabilities of these ciphers and learn how frequency analysis can be employed to break their encryption. The assignment covers the historical context, working principles, encryption process, decryption challenges, and the frequency analysis method for breaking these ciphers.

Shift Cipher

The Shift Cipher, also known as the Caesar Cipher, involves shifting each letter of the plaintext by a fixed number of positions down the alphabet. The encryption process is simple, making it susceptible to attacks. The inherent vulnerabilities of this cipher make it an excellent starting point for understanding encryption weaknesses.

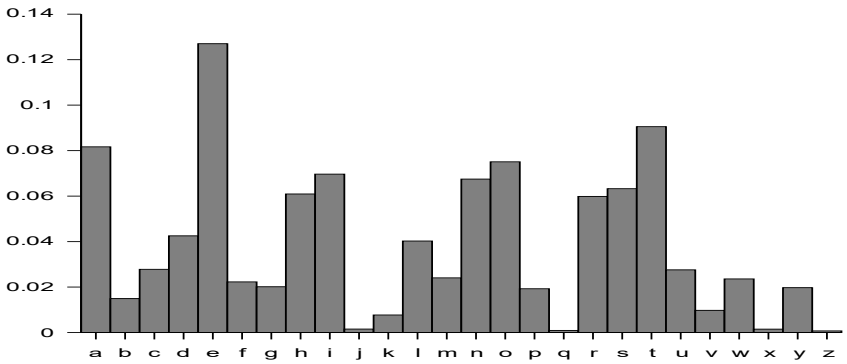




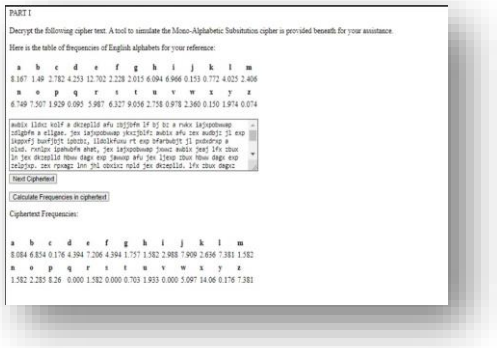


Breaking the Shift Cipher using Frequency Analysis:

Frequency analysis involves analysing the distribution of letters in the ciphertext to deduce the most likely shift value. By observing the frequency of letters in English, we can identify patterns and significantly reduce the key search space. A step-by-step decryption process will be demonstrated using a practical example.



Frequency Analysis Graph



Mono-Alphabetic Substitution Cipher:

The Mono-Alphabetic Substitution Cipher replaces each letter in the plaintext with another letter, number, or symbol. While this seems more secure than the Shift Cipher, it too can be broken using frequency analysis.

Breaking the Mono-Alphabetic Substitution Cipher using Frequency Analysis:

This section will explore how frequency analysis can be adapted to break the Mono-Alphabetic Substitution Cipher. A detailed example will guide through the process of identifying common letters and deducing the substitution key.

Comparative Analysis:

Comparing the vulnerabilities of the Shift Cipher and Mono-Alphabetic Substitution Cipher highlights the importance of understanding encryption weaknesses. The strengths and limitations of frequency analysis will be discussed.

Real-World Relevance:

The historical application of frequency analysis to break ciphers, including its role in pivotal moments, will be examined. The relevance of frequency analysis in modern contexts, such as digital forensics, will also be explored.

Countermeasures:

To mitigate the vulnerabilities of these ciphers, various strategies can be employed. This section introduces basic methods to strengthen the Shift Cipher and Mono-Alphabetic Substitution Cipher, and provides a brief introduction to more advanced encryption techniques.

Conclusion: Summarizing the key takeaways from the assignment, this section emphasizes the historical significance of these ciphers and the importance of understanding their vulnerabilities in the context of modern cryptography.