Instructor's details:

Noor-E Sadman

Adjunct faculty

Department of Computer Science & Engineering

Independent University, Bangladesh

Date:27/07/23

Submitted by:

Name:	***ID:***
Kaushik Day Joy	*1821818*
Sharmin Jaman Niha	*2021865*
MD.Mahbubur Rahman	*2021756*
Jahidul Karim Palash	*2110492*
MD Abu Naushad	*2030295*

Project Topic:
Encryption Algorithm Competition

Algorithm selection: We choose Ceasar Cipher as the encryption and decryption algorithm. Below is the details of this algorithm

Introduction : *Encryption is the process of concealing some data. When plain text is encrypted, it turns into ciphertext, which is unintelligible. Any character of plain text from the predetermined fixed set of characters is replaced by another character from the same set according to a key in a substitution cipher.*

Strength:

- Ease of Use: Substitution ciphers are suitable for basic encryption activities and instructional reasons since they are reasonably easy to comprehend and use.
- Concept Introduction: They provide an introduction to fundamental encryption concepts like mapping and substitution, making them valuable tools for teaching cryptography.
- Obfuscation: A rudimentary level of obfuscation can be provided using substitution ciphers, making it more difficult for untrained onlookers to decipher the message. This might discourage sloppy listening.
- Steganography Component: Substitution ciphers can be used as one component of a steganographic scheme, where hidden

messages are embedded within other data. The use of a cipher can add an extra layer of concealment.

Limitations:

- Vulnerability to Frequency Analysis: Substitution ciphers are susceptible to frequency analysis, which is a weakness..
- Small Key Space: The key space is rather tiny in many substitution ciphers, including the Caesar cypher. For instance, because there are so few keys (shift values) for the Caesar cypher, it is susceptible to brute force attacks
- Lack of Security:In particular, substitution ciphers are not very secure against contemporary cryptographic assaults.

Potential of optimization:Substitution ciphers can be made more secure, less vulnerable by optimizing them.

- Polyalphabetic Substitution:Use numerous substitution rules dependent on the letter's location in the plaintext as opposed to one set substitution rule. Frequency analysis and pattern identification are made more challenging by this method.

- Homophonic Substitution:Give letters with a high frequency a variety of replacements. As a result, the distribution of substitutes becomes more randomly distributed, making frequency analysis less useful.

- Mixed Substitution Rules:Combine various replacement rule types in a single cipher. You could, for instance, combine Caesar, Atbash, and keyword substitution in various areas of the message

Algorithm Analysis:

History:The origins of substitution ciphers can be traced back to ancient civilizations. Polyalphabetic substitution ciphers were later described in 1467 by Leone Battista Alberti in the form of disks. One of the earliest known examples of a substitution cipher is the Atbash cipher, which Hebrews used to encode their alphabet. substitution cipher that replaces each letter with its corresponding letter at the opposite end of the alphabet.

Inventor: The inventor of substitution cipher is Italian cryptographer Giovan Battista Bellaso in 1553. For centuries was attributed to the 16th-century French cryptographer Blaise de Vigenère, who devised a similar cipher in 1586.
operating principles:

Operating Principles:The operating principles of substitution ciphers involve the following key concepts:
Substitution Rule or Key
Alphabet Mapping
One-to-One Mapping
Key Space
Encryption and Decryption
Security and Vulnerabilities
Polyalphabetic Substitution
Modern Substitution Ciphers

computational complexity:

- Encryption Complexity: This is a linear operation that runs in O(n) time, where n is the length of the plaintext.

- Decryption Complexity:It is also a linear operation, similar to encryption, running in O(n) time.
- Brute-Force Attacks: In the case of polyalphabetic substitution ciphers with larger key spaces, brute-force attacks become more time-consuming but can still be feasible if the key space is not sufficiently large

Flowchart Development: