Two Page Report

Tyra Baxter, Hamza Amadu, Alpha Bah, Jire Dada, & Teron Brown

Department of Computer Technology, Bowie State University

CTEC 445: Foundation of Cryptography

Dr. Jackson

April 7, 2025

Encryption is the process of securing sensitive information and data by transforming it into Plaintext that is scrambled using substitution and complex algorithms. This makes sure that only the intended receiver with the correct key can decrypt the sensitive information.

Strengths:

Enhanced ciphers, like AES (Advance Encryption Standards) and RSA, offer strong security with the use of hard to crack algorithms, making them resistant to cryptographic and brute-force attacks by implementing advanced mathematical methods and longer key lengths to guarantee data confidentiality and integrity, providing strong protection for sensitive information.

Weakness:

Despite advanced ciphers strength’s, they are vulnerable to the evolving quantum computing attacks. Also, improper key management or implementation that is exposed can lead to potential data risks.

Historical or modern applications:

Enhanced Cipher has been used for ages in protecting sensitive information. It evolved from simple code changes to complex encryption algorithms. During war times messages were encrypted to protect sensitive information to ensure the message gets to and read by intended receiver. In today's time encryption is being widely used in everyday online tasks like AES encryption secure online banking, messaging, and government data.

Enhanced Ceasar Cipher vs Ceasar Cipher

The Ceasar cipher is a simple encryption technique that uses letter in a plaintext shifted by a fixed number of positions in the alphabet

Enhanced Ceasar cipher consolidate upon the Ceasar cipher by adding more layers of complexity for data security

Important notes

Variable shift means that the letter shift can vary based on the key pattern

Mixed Alphabet custom alphabet can be used

Multiple rounds: data could experience several rounds of encryption with shift key

Integration with other methods: enhanced cipher could work with

Other techniques to improve data security

How could attackers break Enhanced Ceasar Cipher

Frequency analysis: pattern of letter can be used to deduced to shift the key

Brute-force attack: attackers can test all potential keys systematically

Known plaintext attack: common phrase can be compared with the ciphertext to deduce the encryption pattern

Vulnerable key management: stolen key/used pattern can be used to decrypt the ciphertext

Chosen ciphertext attack: attackers could input specific plaintext and observe the result for reverse-engineering

Reflection Phase (Jire)

What we learnt from the two groups collaborations

We learnt the basic understanding of cipher types such as an alphabet cipher typically shows that substitution of letter of the alphabet and that of enhanced cipher further incorporates more complex algorithms and can even use entirely different approaches in the case of modern encryption that is useful in digital security.

Historical importance of the two ciphers and their foundation in the history of cryptography and the evolution of enhanced cipher to reinforce the alphabet cipher for data security.

Application of the two cipher shows that alphabet cipher may still have practical applications in the educational settings while enhanced cipher is indispensable for securing critical information in the online transaction.

Our collaborations help us to understand how cryptography was used to solve the threat in data security. These challenges could be solved by using regular audits, continuous development and to be UpToDate in the advancement of cryptography techniques such as using SHA256 for data encryption.

References

CodeHS. (n.d.). Learn coding with CodeHS. CodeHS. https://codehs.com

Smith, J. (2020). Cryptography and ciphers: A beginner's guide (2nd ed.). Cengage Learning.