COMPARISON OF THE HILL CIPHER AND AFFINE CIPHER ALGORITHMS IN MAINTAINING DATA SECURITY ON E-COMMERCE WEBSITES

Student Name : ONA MAZURA
Student ID : 6404221095

Supervisor : Nurmi Hidayasari, ST., M. Kom

ABSTRACT

User data security is an important aspect of e-commerce systems because it involves sensitive information that is vulnerable to unauthorized access. One method that can be used to protect such data is classical cryptography. This study aims to compare the Hill Cipher and Affine Cipher algorithms in securing user data in a web-based e-commerce system. Both algorithms are implemented in an open-source e-commerce system by encrypting user data in the form of usernames, emails, and passwords before being stored in the database. The evaluation is conducted by analyzing the performance of the encryption and decryption *processes as well as the security of the ciphertext using the Ciphertext-Only Attack (COA) approach and Shannon Entropy. The results show that the Affine Cipher has faster encryption and decryption processing times, while the Hill Cipher produces ciphertext with a higher level of complexity and randomness. COA analysis indicates that the ciphertext generated by both algorithms does not exhibit meaningful patterns. Furthermore, the Shannon Entropy test results show that the Hill Cipher produces an entropy value of 4,55 bits, which falls into the high randomness category, while the Affine Cipher produces an entropy value of 3,60 bits, which is categorized as moderate randomness. Based on these results, it can be concluded that the Affine Cipher excels in terms of time efficiency, whereas the Hill Cipher performs better in generating complex ciphertext. This study is expected to serve as a reference for selecting classical cryptographic algorithms to secure data in web-based e-commerce systems.*

Keywords: *Data Security, Classical Cryptography, Hill Cipher, Affine Cipher, Ciphertext-Only Attack, Shannon Entropy, E-Commerce.*