IMPLEMENTASI ENKRIPSI *CAESAR CIPHER* DAN *VIGENERE CIPHER* UNTUK KEAMANAN DATA PADA *ROUTING* APLIKASI-*DATABASE*

Adzin Hafidh Albar

ABSTRAK

Keamanan data merupakan aspek penting dalam pengembangan perangkat lunak, terutama pada aplikasi yang menangani data pribadi pengguna. Salah satu pendekatan yang umum digunakan untuk menjaga keamanan data adalah kriptografi. Penelitian ini mengimplementasikan dua algoritma kriptografi klasik, yaitu *Caesar Cipher* dan *Vigenere Cipher*, secara bersamaan untuk meningkatkan keamanan data dalam proses komunikasi antara aplikasi dan *database*. Meskipun kedua algoritma ini tergolong sederhana dan memiliki kelemahan jika digunakan secara terpisah, kombinasi keduanya terbukti mampu meningkatkan efektivitas enkripsi data dengan tetap mempertahankan efisiensi sistem. Implementasi dilakukan pada layanan *backend* dengan memodifikasi bagian *controller* agar proses enkripsi dan dekripsi berjalan otomatis. Hasil pengujian menunjukkan bahwa algoritma mampu mengubah plaintext menjadi ciphertext dan sebaliknya dengan tingkat keberhasilan 100% serta waktu proses kurang dari 0,5 detik per iterasi. Proses ini tidak memberikan dampak signifikan terhadap performa sistem secara keseluruhan. Dengan demikian, kombinasi *Caesar Cipher* dan *Vigenere Cipher* dinilai layak diterapkan dalam aplikasi berskala kecil hingga menengah yang tidak membutuhkan sistem kriptografi kompleks namun tetap memerlukan perlindungan data yang andal.

Kata Kunci: keamanan data, kriptografi, *Caesar Cipher*, *Vigenere Cipher*, enkripsi, *backend*.

IMPLEMENTASI ENKRIPSI *CAESAR CIPHER* DAN *VIGENERE CIPHER* UNTUK KEAMANAN DATA PADA *ROUTING* APLIKASI-*DATABASE*

Adzin Hafidh Albar

ABSTRACT

Data security is a critical aspect of software development, particularly for applications that manage users' personal information. One common approach to ensuring data security is through cryptography. This study implements a combination of two classical cryptographic algorithms, Caesar Cipher and Vigenere Cipher, to enhance data protection during communication between applications and databases. Although both algorithms are relatively simple and weak when used individually, their combined application has proven effective in strengthening data encryption while maintaining system efficiency. The implementation is integrated into the backend service by modifying the controller component to automate encryption and decryption processes. Testing results indicate a 100% success rate in converting plaintext to ciphertext and vice versa, with processing times under 0.5 seconds per iteration. Moreover, the encryption and decryption processes do not significantly impact overall system performance. Therefore, the combined use of Caesar Cipher and Vigenère Cipher is considered suitable for small to medium-scale applications that do not require advanced cryptographic systems but still demand reliable data protection.

Keywords*: data security, cryptography, Caesar Cipher, Vigenere Cipher, encryption, backend.*