IMPLEMENTASI ALGORITMA *ADVANCED ENCRYPTION STANDARD* (AES) DAN *ELLIPTIC CURVE CRYPTOGRAPHY* (ECC) UNTUK MENGURANGI KEBOCORAN DATA FILE DOKUMEN PDF DAN DOCX DI PT XYZ

MUHAMMAD FARREL DAVIAZIZ

ABSTRAK

Penelitian ini menjawab tantangan keamanan data di PT XYZ, yang menghadapi risiko kebocoran informasi akibat ketiadaan standar enkripsi level file. Untuk mengatasi celah ini, sebuah sistem pengamanan file berbasis arsitektur enkripsi hibrida dirancang dan diimplementasikan. Sistem ini mengkombinasikan kecepatan algoritma Advanced Encryption Standard (AES-256) untuk enkripsi konten file dengan kekuatan Elliptic Curve Cryptography (ECC) untuk mengamankan kunci sesi AES. Implementasi dilakukan melalui skrip Command Line Interface (CLI) menggunakan bahasa pemrograman Python untuk kemudahan integrasi. Evaluasi efektivitas sistem dilakukan melalui pengujian pada 20 file dokumen (PDF dan DOCX) dengan ukuran bervariasi, berfokus pada performa (waktu eksekusi dan penggunaan memori) serta integritas data (verifikasi hash SHA-256). Hasilnya menunjukkan kinerja yang sangat efisien dan andal. Rata-rata waktu eksekusi untuk enkripsi adalah 0.0259 detik dan dekripsi 0.0332 detik, dengan penggunaan memori puncak rata-rata hanya 35.78 MB. Pengujian integritas data mencapai keberhasilan 100%, dibuktikan dengan kesamaan nilai hash antara file asli dan hasil dekripsi. Penelitian ini menyimpulkan bahwa implementasi hibrida AES-ECC merupakan solusi efektif, efisien, dan praktis untuk mengamankan aset digital sensitif tanpa mengorbankan produktivitas.

Kata Kunci: Enkripsi Hibrida, AES-256, ECC, Keamanan File, Python

IMPLEMENTATION OF ADVANCED ENCRYPTION STANDARD (AES) AND ELLIPTIC CURVE CRYPTOGRAPHY (ECC) ALGORITHMS TO REDUCE DATA LEAKS IN PDF AND DOCX DOCUMENT FILES AT PT XYZ

MUHAMMAD FARREL DAVIAZIZ

ABSTRACT

This research addresses the data security challenges at PT XYZ, which faces the risk of information leakage due to the lack of a file-level encryption standard. To address this vulnerability, a file security system based on a hybrid encryption architecture was designed and implemented. The system combines the speed of the Advanced Encryption Standard (AES-256) algorithm for content encryption with the robustness of Elliptic Curve Cryptography (ECC) for securing the AES session key. The system was implemented as a Command Line Interface (CLI) script using Python, ensuring ease of integration into daily workflows. The system's effectiveness was evaluated by testing 20 document files (PDF and DOCX) of varying sizes, focusing on performance (execution time and memory usage) and data integrity (SHA-256 hash verification). The results showed highly efficient and reliable performance. The average execution time was 0.0259 seconds for encryption and 0.0332 seconds for decryption, with an average peak memory usage of only 35.78 MB. Data integrity tests achieved a 100% success rate, confirmed by identical hash values between the original and decrypted files. This study concludes that the hybrid AES-ECC implementation is an effective, efficient, and practical solution for securing sensitive digital assets without compromising productivity.

Keywords: *Hybrid Encryption, AES-256, ECC, File Security, Python*