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

SKRIPSI

Disusun Oleh:

MUHAMMAD FARREL DAVIAZIZ

NIM. 2110511104

PROGRAM STUDI INFORMATIKA

FAKULTAS ILMU KOMPUTER

UNIVERSITAS PEMBANGUNAN NASIONAL "VETERAN" JAKARTA

2025

PERNYATAAN ORISINALITAS

PERNYATAAN ORISINALITAS

Tugas Akhir ini adalah hasil karya sendiri dan semua sumber baik yang dikutip maupun yang dirujuk telah saya nyatakan dengan benar.

Nama : Muhammad Farrel Daviaziz

NIM : 2110511104

Tanggal : 15 Januari 2026

Bilamana dikemudian hari ditemukan ketidaksesuaian dengan pernyataan saya ini, maka saya bersedia dituntut dan diproses sesuai dengan ketentuan yang berlaku.

Jakarta, 15 Januari 2026

Yang Menyatakan

Muhammad Farrel Daviaziz

PERNYATAAN PERSETUJUAN PUBLIKASI TUGAS AKHIR UNTUK KEPENTINGAN AKADEMIS

PERNYATAAN PERSETUJUAN PUBLIKASI TUGAS AKHIR UNTUK KEPENTINGAN AKADEMIS

Sebagai civitas akademika Universitas Pembangunan Nasional Veteran Jakarta, saya yang bertanda tangan dibawah ini :

Nama	: Muhammad Farrel Daviaizz
NIM	: 2110511104
Fakultas	: Ilmu Komputer
Program Studi	: S-1 Informatika

Demi pengembangan ilmu pengetahuan, menyetujui untuk memberikan kepada Universitas Pembangunan Nasional Veteran Jakarta Hak bebas royalti non-eksklusif (Non-exclusive Royalti free right) atas skripsi saya yang berjudul :

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

Dengan Hak bebas royalti ini Universitas Pembangunan Nasional Veteran Jakarta berhak menyimpan, mengalih media/memformatkan, mengelola dalam bentuk pangkalan data (basis data), merawat dan mempublikasikan skripsi saya selama tetap mencantumkan nama saya sebagai penulis dan sebagai pemilik hak cipta. Demikian pernyataan ini saya buat dengan sebenarnya.

Dibuat di: Jakarta

Pada tanggal : 15 Januari 2026

Yang Menyatakan

Muhammad Farrel Daviaziz

LEMBAR PENGESAHAN

LEMBAR PENGESAHAN

Judul	:	Implementasi Algoritma Advanced Encryption Standard (AES) dan Elliptic Curve Cryptography (ECC) untuk mengurangi kebocoran data File Dokumen PDF dan Docx di PT XYZ
Nama	:	Muhammad Farrel Daviaziz
NIM	:	2110511104
Prodi	:	Informatika

Disetujui oleh :

Penguji 1:
Jayanta, S.Kom., M.Si

Penguji 2:
Hamonangan Kinantan P., S.T, MT.

Pembimbing 1:
Henki Bayu Seta,
S.Kom., MTI.

Pembimbing 2:
Novi Trisman Hadi, S.Pd., M.Kom.

Diketahui oleh:

Koordinator Program Studi:
Ridwan Raafi'udin, S.Kom.,
M.Kom
NIP. 198805022021211001

Dekan Fakultas Ilmu Komputer:
Prof. Dr. Ir. Supriyanto, S.T., M.Sc., IPM
NIP. 197605082003121002

Tanggal Ujian Tugas
Akhir : 5 Januari 2026

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*

KATA PENGANTAR

Puji dan syukur penulis panjatkan kepada Tuhan Yang Maha Esa, atas segala rahmat-Nya sehingga Tugas Akhir ini berhasil diselesaikan. Tugas Akhir ini dilakukan dalam bentuk skripsi, dengan judul "IMPLEMENTASI ALGORITMA *ADVANCED ENCRYPTION STANDARD* (AES) DAN *ELLIPTIC CURVE CRYPTOGRAPHY* (ECC) UNTUK MENGURANGI KEBOCORAN DATA FILE DOKUMEN PDF DAN DOCX DI PT XYZ". Selama pelaksanaan perkuliahan dan penyelesaian tugas akhir ini, tentu tak lepas dari dukungan dan bimbingan dari banyak pihak, sehingga penulis mengucapkan terima kasih banyak kepada :

1. Kedua Orang Tua dan seluruh Keluarga Besar, terima kasih atas dukungan dan doanya selama ini.
2. Ibu Nindy Irzavika, S.SI., M.T. , Selaku dosen pembimbing akademik.
3. Bapak Henki Bayu Seta, S.Kom., MTI. selaku dosen pembimbing 1 dan Bapak Novi Trisman Hadi, S. Pd., M.Kom selaku dosen pembimbing 2 yang telah membimbing dan memberikan saran dalam penyusunan penelitian ini.
4. Bapak Dr. Ridwan raafi udin, S.Kom, M.Kom., selaku Koordinator Program studi S1 Informatika.
5. Teman-teman penulis yang telah menjadi support system selama ini.

Akhir kata penulis mengucapkan terima kasih kepada semua pihak yang terlibat dan berharap semoga Tuhan yang maha esa membalas semua kebaikan yang telah diberikan.

Jakarta, November 2025
Muhammad Farrel Daviaziz
NIM. 2110511104

DAFTAR ISI