PENGEMBANGAN APLIKASI ENKRIPSI FILE DESKTOP YANG AMAN DAN INTUITIF MENGGUNAKAN ALGORITMA AES-GCM BERBASIS PYTHON

SKRIPSI

Diajukan untuk memenuhi salah satu syarat mencapai derajat Sarjana

Program Studi Teknik Komputer

disusun oleh

MUHAMMAD AZMI TASIRUL HAQ

18.83.0241

Kepada

FAKULTAS ILMU KOMPUTER

UNIVERSITAS AMIKOM YOGYAKARTA

YOGYAKARTA

2025

PENGEMBANGAN APLIKASI ENKRIPSI FILE DESKTOP YANG AMAN DAN INTUITIF MENGGUNAKAN ALGORITMA AES-GCM BERBASIS PYTHON

SKRIPSI

untuk memenuhi salah satu syarat mencapai derajat Sarjana

Program Studi *Teknik Komputer*

disusun oleh

MUHAMMAD AZMI TASIRUL HAQ

18.83.0241

Kepada

FAKULTAS ILMU KOMPUTER

UNIVERSITAS AMIKOM YOGYAKARTA

YOGYAKARTA

2025

HALAMAN PERSETUJUAN

SKRIPSI

PENGEMBANGAN APLIKASI ENKRIPSI FILE DESKTOP YANG AMAN DAN INTUITIF MENGGUNAKAN ALGORITMA AES-GCM BERBASIS PYTHON

yang disusun dan diajukan oleh

Muhammad Azmi Tasirul Haq

18.83.0241

telah disetujui oleh Doseh Pembimbing Skripsi
pada tanggal 25 Juli 2025

Dosen Pembimbing,

Wahid Miftahul Ashari, S.Kom., M.T.
NIK. 190302452

HALAMAN PENGESAHAN

SKRIPSI

PENGEMBANGAN APLIKASI ENKRIPSI FILE DESKTOP YANG AMAN DAN INTUITIF MENGGUNAKAN ALGORITMA AES-GCM BERBASIS PYTHON

yang disusun dan diajukan oleh

Muhammad Azmi Tasirul Haq

18.83.0241

Telah dipertahankan di depan Dewan Penguji
pada tanggal 25 Juli 2025

Susunan Dewan Penguji

Nama Penguji	Tanda Tangan
Senie Destya, M.Kom. **NIK. 190302312**	
Muhammad Koprawi, S.Kom., M.Eng. **NIK. 190302454**	
Wahid Miftahul Ashari, S.Kom., M.T. **NIK. 190302452**	

Skripsi ini telah diterima sebagai salah satu persyaratan
untuk memperoleh gelar Sarjana Komputer
Tanggal 25 Juli 2025

DEKAN FAKULTAS ILMU KOMPUTER

Prof. Dr. Kusrini, M.Kom.
NIK. 190302106

HALAMAN PERNYATAAN KEASLIAN SKRIPSI

Yang bertandatangan di bawah ini,

Nama mahasiswa : Muhammad Azmi Tasirul Haq
NIM : 18.83.0241

Menyatakan bahwa Skripsi dengan judul berikut:

Pengembangan Aplikasi Enkripsi File Dekstop Yang Aman dan Intuitif Menggunakan Algoritma AES-GCM Berbasis Python

Dosen Pembimbing : Wahid Miftahul Ashari, S.Kom., M.T

1. Karya tulis ini adalah benar-benar ASLI dan BELUM PERNAH diajukan untuk mendapatkan gelar akademik, baik di Universitas AMIKOM Yogyakarta maupun di Perguruan Tinggi lainnya.
2. Karya tulis ini merupakan gagasan, rumusan dan penelitian SAYA sendiri, tanpa bantuan pihak lain kecuali arahan dari Dosen Pembimbing.
3. Dalam karya tulis ini tidak terdapat karya atau pendapat orang lain, kecuali secara tertulis dengan jelas dicantumkan sebagai acuan dalam naskah dengan disebutkan nama pengarang dan disebutkan dalam Daftar Pustaka pada karya tulis ini.
4. Perangkat lunak yang digunakan dalam penelitian ini sepenuhnya menjadi tanggung jawab SAYA, bukan tanggung jawab Universitas AMIKOM Yogyakarta.
5. Pernyataan ini SAYA buat dengan sesungguhnya, apabila di kemudian hari terdapat penyimpangan dan ketidakbenaran dalam pernyataan ini, maka SAYA bersedia menerima SANKSI AKADEMIK dengan pencabutan gelar yang sudah diperoleh, serta sanksi lainnya sesuai dengan norma yang berlaku di Perguruan Tinggi.

Yogyakarta, <tanggal lulus ujian skripsi>

Yang Menyatakan,

Muhammad Azmi Tasirul Haq

HALAMAN PERSEMBAHAN

Dengan mengucap syukur kepada Allah S.W.T, Tuhan Yang Maha Esa. Alhamdulillah , penelitian ini selesai dan kupersembahkan untuk orang-orang terkasih:

Anisa Suharianti, Terima kasih telah menjadi penyemangat terbaik dan sumber tawa di hari-hari terberatku. Perjuangan ini lebih bermakna dengan kehadiranmu.

Keluarga Tercinta, Bapak dan Ibuku, terima kasih atas cinta, pengorbanan, dan doa yang tak pernah lekang oleh waktu. Inilah bukti kecil baktiku untuk kalian.

Diriku Sendiri, Terima kasih sudah bertahan. Lelahmu hari ini adalah kemenangan.

Karya ini tak akan selesai tanpa bimbingan dari Bapak **Wahid Miftahul Ashari, S.Kom., M.T.** Terima kasih atas ilmu dan kesabarannya selama membimbing.

KATA PENGANTAR

Puji syukur penulis panjatkan ke hadirat Allah SWT atas segala rahmat, hidayah, dan karunia-Nya yang melimpah. Dalam kesempatan ini, penulis ingin menyampaikan rasa syukur dan terima kasih yang setinggi-tingginya kepada semua pihak yang telah memberikan dukungan, bantuan, dan kontribusi dalam penyelesaian skripsi ini. Pertama-tama, penulis mengucapkan terima kasih yang tak terhingga kepada Wahid Miftahul Ashari, S.Kom., M.T sebagai pembimbing skripsi penulis. Terima kasih atas bimbingan, pengarahan, dan pengawasan yang luar biasa selama proses penelitian dan penulisan skripsi ini. Wahid Miftahul Ashari, S.Kom., M.T telah memberikan panduan yang sangat berharga, wawasan yang mendalam, dan dorongan yang tak terhingga bagi penulis dalam menyelesaikan skripsi ini. Akhir kata, penulis menyampaikan permohonan maaf apabila terdapat kekurangan dalam penulisan skripsi ini. Penulis dengan tulus menerima kritik dan saran yang membangun untuk peningkatan di masa mendatang.

Yogyakarta, <tanggal bulan tahun>
Penulis

DAFTAR ISI

DAFTAR TABEL

DAFTAR GAMBAR

DAFTAR LAMPIRAN

DAFTAR LAMBANG DAN SINGKATAN

AES	Advanced Encryption Standard
GCM	Galois/Counter Mode
AEAD	Authenticated Encryption with Associated Data
KDF	Key Derivation Function
HSM	Hardware Security Module
CBC	Cipher Block Chaining
ECB	Electronic Code Book
MAC	message authentication codes

DAFTAR ISTILAH

Vektor	besaran yang mempunyai arah
Eigen Value	akar akar persamaan

INTISARI

Di tengah banyaknya insiden siber di Indonesia, seperti serangan ransomware terhadap Pusat Data Nasional dan kebocoran data masif, kepercayaan publik terhadap keamanan data terpusat menurun. Kondisi ini menciptakan kebutuhan mendesak akan alat keamanan yang memberdayakan pengguna untuk melindungi data mereka secara mandiri. Penelitian ini bertujuan untuk mengembangkan aplikasi enkripsi file desktop yang aman, intuitif, dan dapat diakses oleh pengguna non-teknis.

Metode penelitian yang digunakan adalah Model Prototype, yang memungkinkan pengembangan iteratif berdasarkan umpan balik pengguna. Aplikasi dibangun menggunakan bahasa pemrograman Python dengan pustaka Tkinter untuk antarmuka pengguna grafis (GUI) dan pustaka cryptography untuk logika inti. Algoritma yang diimplementasikan adalah Advanced Encryption Standard (AES) dengan mode operasi Galois/Counter Mode (GCM) untuk memberikan jaminan kerahasiaan dan integritas data secara simultan. Keamanan kata sandi diperkuat dengan fungsi derivasi kunci PBKDF2-HMAC.

Hasil pengujian diharapkan menunjukkan aplikasi berhasil mengenkripsi dan mendekripsi berbagai jenis file dengan kinerja yang efisien. Pengujian fungsional memvalidasi bahwa semua fitur berjalan sesuai harapan, termasuk penanganan error dan deteksi file yang dimodifikasi, yang membuktikan efektivitas mode GCM. Pengujian usabilitas oleh pengguna non-teknis mengonfirmasi bahwa antarmuka aplikasi mudah dipahami dan dioperasikan. Hasil penelitian ini adalah sebuah perangkat lunak sumber terbuka yang fungsional dan dapat dimanfaatkan oleh masyarakat luas untuk meningkatkan keamanan data digital pribadi mereka.

Kata kunci: Enkripsi, AES-GCM, Python, Keamanan Data, Aplikasi Desktop.

ABSTRACT

Amid numerous cyber incidents in Indonesia, such as ransomware attacks on the National Data Center and massive data breaches, public trust in centralized data security has declined. This situation creates an urgent need for security tools that empower users to independently protect their data. This research aims to develop a secure, intuitive, and accessible desktop file encryption application for non-technical users.

The research method used is the Prototype Model, which allows iterative development based on user feedback. The application is built using the Python programming language with the Tkinter library for the graphical user interface (GUI) and a cryptography library for the core logic. The implemented algorithm is the Advanced Encryption Standard (AES) with Galois/Counter Mode (GCM) operation mode to guarantee data confidentiality and integrity simultaneously. Password security is strengthened with the PBKDF2-HMAC key derivation function.

Test results are expected to demonstrate the application's successful encryption and decryption of various file types with efficient performance. Functional testing validated that all features performed as expected, including error handling and modified file detection, demonstrating the effectiveness of GCM mode. Usability testing by non-technical users confirmed that the application's interface is easy to understand and operate. The result of this research is functional open-source software that can be used by the general public to enhance the security of their personal digital data.

Keyword: *Encryption, AES-GCM, Python, Data Security, Desktop Applications*.