STUDI LITURATUR: PERANCANGAN APLIKASI ENKRIPSI DAN DEKRIPSI FILE MENGGUNAKAN ALGORITMA AES-256 BERBASIS STREAMLIT

1. Pendahuluan

Dalam era digital, perlindungan dokumen penting seperti tugas akademik dan laporan kerja menjadi prioritas untuk menghindari risiko kebocoran data. Kriptografi modern, khususnya *Advanced Encryption Standard* (AES), merupakan solusi fundamental yang diadopsi secara global untuk menjaga kerahasiaan data. Namun, efektivitas sistem keamanan tidak hanya bergantung pada algoritma, tetapi juga pada kemudahan akses bagi pengguna non-teknis melalui antarmuka yang intuitif. Tinjauan ini menganalisis implementasi AES-256 menggunakan framework Streamlit untuk menyediakan solusi keamanan file lokal yang praktis dan kuat.

2. Landasan Teori

Untuk membangun aplikasi yang kokoh, diperlukan pemahaman mendalam mengenai mekanisme enkripsi blok dan teknik penurunan kunci berbasis kata sandi.

2.1 Advanced Encryption Standard (AES-256)

AES merupakan algoritma *block cipher* simetris yang bekerja pada blok data berukuran tetap 128-bit. Varian AES-256 menggunakan panjang kunci 256-bit, yang menawarkan ruang kunci sangat besar sehingga resisten terhadap serangan *brute-force*. Algoritma ini dipilih karena keseimbangan antara kekuatan keamanan dan performa untuk penggunaan sehari-hari.

2.2 Mode Operasi: Galois/Counter Mode (GCM)

Aplikasi ini menggunakan mode AES-GCM, sebuah mode operasi yang menyediakan dua fungsi sekaligus:

- **Kerahasiaan (Confidentiality):** Mengenkripsi isi file sehingga tidak dapat dibaca tanpa kunci yang benar.
- **Autentikasi Integritas:** Menjamin bahwa file tidak dimodifikasi secara tidak sah selama penyimpanan. Jika data diubah, proses dekripsi akan gagal.

2.3 Penurunan Kunci: PBKDF2-HMAC-SHA256

Karena pengguna menggunakan password (teks) dan bukan kunci biner murni, diperlukan fungsi penurunan kunci. PBKDF2 (*Password-Based Key Derivation Function 2*) digunakan dengan penambahan *salt* acak dan iterasi tinggi untuk menghasilkan kunci AES-256 yang aman dan sulit ditebak melalui serangan kamus.

2.4 Framework Streamlit

Streamlit adalah framework berbasis Python yang memungkinkan pengembangan aplikasi web interaktif dengan cepat. Framework ini menyediakan komponen unggah (*upload*) dan unduh (*download*) file secara langsung di browser, sehingga pengguna tidak perlu menggunakan perintah terminal (*command line*) yang rumit.

3. Tinjauan Pustaka Terdahulu: Sintesis Kritis

Peneliti & Tahun	Fokus Penelitian	Hasil Empiris Kunci	Analisis & Kontribusi
Stallings (2017)	Prinsip Keamanan Jaringan	Menekankan pentingnya kriptografi kunci simetris untuk efisiensi data besar.	Dasar teori penggunaan AES dalam skala penggunaan umum.
Ferguson dkk (2010)	Desain Rekayasa Kriptografi	Menggarisbawahi pentingnya manajemen *nonce* dan *salt* dalam sistem keamanan.	Memberikan fondasi praktis untuk implementasi *salt* dan *nonce* pada aplikasi.
NIST (2007 & 2010)	Standardisasi Mode GCM & PBKDF2	Menetapkan standar global untuk keamanan data dan penurunan kunci berbasis password.	Memvalidasi penggunaan GCM dan PBKDF2 sebagai standar keamanan tinggi.

4. Analisis dan Sintesis: Keunggulan dan Tantangan

4.1 Keunggulan Sistem

- **Keamanan Berlapis:** Kombinasi AES-256 dan mode GCM memberikan perlindungan kerahasiaan sekaligus integritas data.
- **Kemudahan Akses:** Penggunaan Streamlit menghilangkan hambatan teknis bagi pengguna awam karena proses dilakukan melalui antarmuka web.
- **Performa Stabil:** Pengujian menunjukkan bahwa *overhead* waktu untuk file berukuran hingga 18 MB (sekitar 5 detik) masih berada pada rentang yang dapat diterima.

4.2. Tantangan dan Kelemahan

- **Ketergantungan pada Password:** Keamanan sistem sepenuhnya bergantung pada kekuatan password yang dibuat pengguna.
- **Manajemen Kunci Lokal:** Prototipe saat ini masih mengandalkan penyimpanan kunci secara lokal oleh pengguna itu sendiri.

5. Kesimpulan

Aplikasi enkripsi dan dekripsi file berbasis Streamlit menggunakan algoritma AES-256 terbukti layak sebagai solusi sederhana untuk meningkatkan keamanan data lokal. Penggunaan mode GCM dan PBKDF2 memastikan standar keamanan yang kuat, sementara antarmuka web memberikan pengalaman pengguna yang lebih baik dibandingkan aplikasi berbasis terminal. Pengembangan masa depan disarankan mencakup manajemen password yang lebih aman dan integrasi dengan layanan penyimpanan awan.