BAB V
PENUTUP

5.1 Kesimpulan

Berdasarkan Hasil dan Tahapan Penelitian yang telah dilakukan, maka dapat ditarik kesimpulan sebagai berikut:

1. Skrip pengamanan file telah berhasil diimplementasikan untuk menjalankan fungsi enkripsi dan dekripsi dokumen dengan menggunakan kombinasi algoritma AES-256 untuk enkripsi konten dan ECC untuk pengamanan kunci. Keberhasilan ini dicapai melalui implementasi arsitektur enkripsi hibrida yang menggabungkan keunggulan dari dua algoritma berbeda. Algoritma simetris AES-256 digunakan untuk tugas enkripsi konten file secara efisien, sementara algoritma asimetris ECC diimplementasikan secara spesifik untuk mengamankan kunci sesi AES. Alur kerja terpadu ini terbukti secara konsisten mampu mengubah dokumen asli menjadi format ciphertext yang aman dan kemudian mendekripsinya kembali ke bentuk semula tanpa kesalahan.
2. Hasil pengujian performa secara kuantitatif memberikan bukti empiris yang kuat untuk klaim ini. Secara spesifik, waktu eksekusi rata-rata untuk keseluruhan proses enkripsi pada 20 file uji adalah 0.0259 detik, sementara untuk proses dekripsi adalah 0.0332 detik. Kecepatan pemrosesan yang tinggi ini didukung oleh jejak sumber daya yang sangat rendah; penggunaan memori puncak rata-rata tercatat hanya 35.78 MB. Kombinasi latensi yang minimal dan penggunaan memori yang ringan memastikan bahwa skrip dapat diadopsi tanpa menjadi hambatan produktivitas atau memerlukan perangkat keras dengan spesifikasi tinggi. Efisiensi ini, terutama jika dibandingkan dengan alternatif algoritma asimetris untuk enkripsi data bervolume besar sebagaimana dibahas dalam studi oleh Alvi Sholikhatin et al. (2022), secara meyakinkan menunjukkan bahwa solusi yang diusulkan tidak hanya aman tetapi juga sangat praktis.

3. Berdasarkan pengujian integritas menggunakan perbandingan hash SHA-256 secara meyakinkan menunjukkan bahwa tidak ada kehilangan atau modifikasi data selama siklus enkripsi-dekripsi. Hasil verifikasi yang 100% identik antara file asli dan file hasil dekripsi pada 20 file uji (PDF dan DOCX) membuktikan bahwa implementasi kriptografi bersifat *lossless* dan akurat.

5.2 Saran

Berdasarkan kesimpulan yang telah ditarik dan potensi pengembangan dari solusi yang ada, berikut adalah beberapa saran yang dapat dipertimbangkan untuk penelitian selanjutnya:

1. Pengembangan Sistem Manajemen Kunci (KMS): Penelitian di masa depan dapat berfokus pada pengembangan sistem manajemen kunci yang terpusat untuk mengatasi tantangan pengelolaan kunci privat ECC secara individual, terutama dalam skala organisasi yang besar.
2. Optimalisasi untuk File Berukuran Sangat Besar: Untuk menangani file berukuran sangat besar (ratusan MB atau GB), penelitian di masa depan dapat mengeksplorasi teknik *streaming encryption*, di mana file dienkripsi per-bagian (*chunk-by-chunk*) tanpa perlu memuat seluruhnya ke dalam RAM, sehingga dapat meningkatkan efisiensi memori secara signifikan.
3. Integrasi dengan Tanda Tangan Digital (*Digital Signature*): Untuk menambah lapisan keamanan, fungsionalitas skrip dapat diperluas dengan mengintegrasikan algoritma tanda tangan digital (misalnya, ECDSA - *Elliptic Curve Digital Signature Algorithm*). Ini tidak hanya akan menjamin kerahasiaan (enkripsi) dan integritas (hash), tetapi juga autentisitas (siapa pengirimnya) dan non-repudiasi (pengirim tidak dapat menyangkal telah mengirimnya).