JIKA (Jurnal Informatika) Universitas Muhammadiyah Tangerang
Vol 10, No 1, Januari 2026, pp 43-50

P ISSN : 2549-0710
E ISSN : 2722-2713

PENERAPAN KRIPTOGRAFI UNTUK PENGAMANAN DOKUMEN NASABAH ASURANSI MENGGUNAKAN METODE AES-128

Nico Nandika[1)], Rizky Pradana[2)], Indah Puspasari Handayani[3)]

[1,2]Teknik Informatika Fakultas Teknologi Informasi, Universitas Budi Luhur, Jl. Ciledug Raya – DKI Jakarta
[3]Sistem Informasi Fakultas Teknologi Informasi, Universitas Budi Luhur, Jl. Ciledug Raya – DKI Jakarta
Co Responden Email: indah.puspasari@budiluhur.ac.id

Article history
Received 10 Oct 2025
Revised 23 Dec 2025
Accepted 14 Jan 2026
Available online 31 Jan 2026

Keywords
Cryptography,
Encryption,
AES-128,
Data Security,
Document Application

Abstract

In the digital era, protecting customer data is crucial, especially for PT Asuransi Jiwa Astra, which manages confidential documents. The rise of data leakage demands a strong security system. This research develops a document encryption and decryption application using the 128-bit Advanced Encryption Standard (AES) algorithm to overcome these problems. The methods used include designing, implementing, and testing the application, focusing on functionality, performance, and data security. The application supports automatic and secure document upload, encryption-decryption, storage, and download. The test results show that the functions run optimally with 100% success. The encryption process averaged 3.35 seconds per file (max. 3MB). In terms of security, AES-128 proved effective in protecting data confidentiality up to 99%. Thus, this system is feasible to be used as a digital document security solution at PT Asuransi Jiwa Astra.

Riwayat
Diterima 10 Okt 2025
Revisi 23 Des 2025
Disetujui 14 Jan 2026
Terbit online 31 Jan 2026

Kata Kunci
Kriptografi,
Enkripsi,
AES-128,
Keamanan Data,
Aplikasi Dokumen

Abstrak

Dalam era digital, perlindungan data nasabah menjadi krusial, terutama bagi PT Asuransi Jiwa Astra yang mengelola dokumen rahasia. Maraknya kebocoran data menuntut sistem keamanan kuat. Penelitian ini mengembangkan aplikasi enkripsi dan dekripsi dokumen menggunakan algoritma *Advanced Encryption Standard* (AES) 128-bit untuk mengatasi masalah tersebut. Metode yang digunakan meliputi perancangan, implementasi, dan pengujian aplikasi, berfokus pada fungsionalitas, performa, dan keamanan data. Aplikasi ini mendukung unggah, enkripsi-dekripsi, penyimpanan, serta unduh dokumen secara otomatis dan aman. Hasil pengujian menunjukkan fungsi berjalan optimal dengan keberhasilan 100%. Proses enkripsi rata-rata 3,35 detik per *file* (maks. 3MB). Dari sisi keamanan, AES-128 terbukti efektif melindungi kerahasiaan data hingga 99%. Dengan demikian, sistem ini layak digunakan sebagai solusi pengamanan dokumen *digital* di PT Asuransi Jiwa Astra.

PENDAHULUAN

Pada masa digitalisasi saat ini, tanpa disadari sebagian besar aktivitas keseharian sudah dimudahkan oleh teknologi yang terus mengalami perkembangan. Perubahan positif ini banyak sekali dirasakan, dari mulai beberapa pekerjaan, komunikasi, belanja dan belajar yang dapat dilakukan secara *online* (Baqis & Nasution, 2025). Kemudahan yang selalu ditawarkan oleh teknologi ini, juga dimanfaatkan masyarakat, contohnya adalah sebagian besar masyarakat mempercayakan *platform* sebagai media penyimpanan data yang sifatnya publik, maupun data yang sifatnya pribadi atau rahasia. Namun keamanan data selalu menjadi permasalahan, terutama kesadaran masyarakat akan perlindungan data pribadinya. Perlu dipahami bahwa keamanan data termasuk dalam urusan informasi pribadi, yang tentunya sangat sensitif untuk dipublikasikan ke pihak lain, baik secara umum maupun secara sembunyi.

Tetapi kebocoran data tersebut masih sering terjadi di Indonesia, sebagai contoh: tahun 2020 jutaan data pengguna tokopedia mengalami kebocoran data, tahun 2021 sekitar 13 juta data pengguna bukalapak dilaporkan terdampak dari kebocoran data yang terjadi, dan yang lebih fatal adalah pada tahun 2021 tokotalk mengalami kebocoran data sebanyak

91 juta akun penggunanya (Suari & Sarjana, 2023). Selain itu, mengadopsi laporan data privasi index tahun 2023, terjadi kenaikan 35% pencurian identitas dari *platform* media sosial (Nopriadi, 2024). Dari keempat kasus kebocoran data diatas telah membuktikan bahwa batasan privasi semakin berkurang, walaupun teknologi informasi mengalami kemajuan (Hasibuan & Putri, 2024).

Di Indonesia, kasus kebocoran data telah terjadi berulang kali, baik di sektor publik maupun swasta. Salah satu kasus yang mencuat adalah kebocoran data 279 juta peserta BPJS Kesehatan pada Mei 2021, yang mencakup Nomor Induk Kependudukan (NIK), nama, alamat, dan nomor telepon (Nugraha et al., 2025). Selain itu, pada Juli 2021, data 2 juta nasabah BRI *Life* diduga bocor dan dijual di forum daring, mencakup informasi sensitif seperti KTP dan polis asuransi (Bhagaskara & Priyanto, 2024). Kasus-kasus ini menunjukkan kerentanan sistem keamanan siber di Indonesia dan menimbulkan dampak yang serius terhadap privasi individu serta kepercayaan publik, sedangkan perlu disadari bahwa memperoleh keamanan data juga salah satu hak dari semua orang (Ramadhan et al., 2023). Kebocoran data tidak hanya menyebabkan kerugian finansial, tetapi juga meningkatkan risiko pencurian identitas, penipuan, dan ancaman keamanan nasional. Menurut Kementerian Komunikasi dan Informatika, dari 2019 hingga Mei 2024, terdapat 124 kasus dugaan pelanggaran data pribadi di Indonesia dengan jumlah sekitar 205.320.000 data, mayoritas berupa kebocoran data (Mediana, 2024). Meskipun regulasi Perlindungan Data Pribadi (PDP) melalui UU No. 27 Tahun 2022 telah diberlakukan untuk mengatasi masalah ini, implementasinya masih menghadapi tantangan, seperti kurangnya infrastruktur keamanan siber yang memadai dan rendahnya kesadaran akan pentingnya perlindungan data.

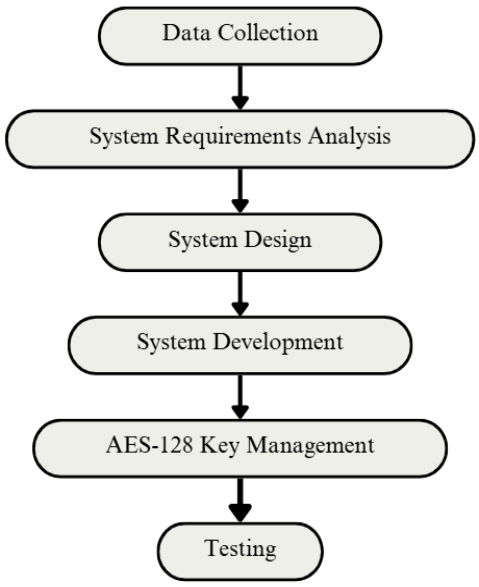
Ancaman terhadap data semakin kompleks sejalan dengan pesatnya perkembangan teknologi dan metode serangan yang semakin canggih. Jika diperhatikan, keamanan data ini menjadi momok tahunan yang selalu saja berulang. Maka, perlu adanya pengembangan teknologi yang dapat menjamin *confidentiality, integrity* dan *availability* (Handoyo et al., 2025). Salah satu cara pengamanan data adalah dengan kriptografi, yang merupakan teknik pengamanan informasi melalui enkripsi dan dekripsi, memainkan peran penting dalam melindungi kerahasiaan, integritas, dan autentikasi data (Nanda et al., 2023). Sistem kriptografi telah digunakan dalam berbagai aplikasi, seperti transaksi perbankan *online*, komunikasi rahasia, dan penyimpanan data yang sensitif. Salah satu algoritma kriptografi adalah *Advance Encryption Standard* (AES), yang mempunyai kunci enkripsi dan panjang bit yang berbeda (Wachid Hidayatulloh et al., 2023). *Advance Encryption Standard* (AES) terbukti efektif dan dapat diterima pada beberapa organisasi untuk perlindungan data secara aman, keamanan jaringan dan penjagaan peranglat lunak (Rizky et al., 2024).

PT Asuransi Jiwa Astra, merupakan salah satu perusahaan asuransi yang memiliki reputasi baik di Indonesia, mengelola berbagai dokumen nasabah yang bersifat sensitif, seperti data pribadi, informasi keuangan, dan dokumen kontrak asuransi. Keamanan dokumen-dokumen ini sangat penting untuk menjaga privasi nasabah, mematuhi regulasi perlindungan data yang telah di atur dan berada di bawah pengawasan Otoritas Jasa Keuangan (OJK), serta mencegah potensi penyalahgunaan informasi. PT Asuransi Jiwa Astra belum pernah mengalami kebocoran data, akan tetapi PT Asuransi Jiwa Astra menghadapi tantangan signifikan dalam menjaga kerahasiaan, integritas, dan ketersediaan dokumen digital. Tanpa perlindungan yang memadai, data sensitif yang disimpan oleh PT Asuransi Jiwa Astra dapat dengan mudah menjadi target bagi penjahat siber, yang dapat berdampak buruk pada kepercayaan masyarakat dan operasional organisasi. Terlebih, pelaku dapat melakukan aksinya ke siapa saja yang terhubung internet, untuk pencurian data, pemerasan dan sejenisnya (Ihtisyamuddin et al., 2024). Maka, perlu adanya pembenahan dengan mengoptimalkan pengamanan informasi atau data untuk menghadapi kejahatan siber (Butarbutar, 2023).

Dalam mengamankan data, algoritma AES akan difokuskan untuk melancarkan penelitian ini. Penerapan kriptografi, khususnya AES-128, masih menghadapi tantangan seperti pengelolaan kunci enkripsi, performa sistem, dan integrasi dengan infrastruktur teknologi informasi yang ada. Berdasarkan hal tersebut,

kajian ini dilakukan guna menganalisis dan mengimplementasikan metode AES-128 dalam mengamankan dokumen nasabah di PT Asuransi Jiwa Astra, dengan fokus pada efisiensi, keamanan, dan kemudahan integrasi, dengan serangkaian operasi linier dan non-linier pada setiap *data block* (Abdullah et al., 2025). Penelitian sebelumnya di Indonesia telah menunjukkan berbagai pendekatan untuk meningkatkan keamanan data digital, sebagai contoh penelitian dengan judul "Implementasi Sistem Keamanan *File* Menggunakan Algoritma AES Untuk Mengamankan *File* Pribadi" menunjukkan hasil algoritam AES mampu melindungi *file* dengan baik, sehingga dapat dapat dijadikan sebagai penyelesaian yang efektif dalam pengamanan file dari berbagai serangan (Saripa, 2024). AES- 128 menawarkan perlindungan data yang optimal menggunakan kompleksitas komputasi yang relatif rendah, sehingga cocok diterapkan pada sistem pengelolaan dokumen nasabah di PT Asuransi Jiwa Astra.

METODE PENELITIAN



Gambar 1. Tahapan penelitian

Gambar 1 merupakan tahapan penelitian yang dilakukan, adapun penjelesan lebih detilnya adalah sebagai berikut:

a. *Data Collection*
Pengumpulan data yang digunakan merupakan data primer dan data sekunder. Data primer didapatkan langsung dari sumber asli (Sulung & Muspawi, 2024), dengan melakukan *interview* dan observasi atau pengamatan langsung dokumen nasabah yang ada di PT Asuransi Jiwa Astra untuk mengidentifikasi potensi risiko dan kebutuhan keamanan. Data sekunder yang didapatkan dari penelitian terdahulu (Handayani & Pradana, 2023), dilakukan *literature review* dengan mengumpulkan informasi dari berbagai sumber, termasuk jurnal ilmiah, buku, dan artikel, untuk memahami konsep dasar kriptografi, algoritma AES-128, serta standar keamanan data yang relevan di industri asuransi.

b. *System Requirement Analysis*
Mendefinisikan fungsionalitas utama yang diperlukan, seperti unggah dokumen, enkripsi, dekripsi, penyimpanan aman, dan unduh dokumen.

c. *System Design*
Membuat arsitektur sistem, rancangan basis data, dan antarmuka pengguna (UI/UX) yang intuitif. Perancangan ini berfokus pada integrasi algoritma AES-128 dalam alur kerja yang sudah ada.

d. *AES-128 Key Management*
Merancang mekanisme untuk pembangkitan, penyimpanan, dan pengelolaan kunci AES-128 secara aman untuk menjamin kerahasiaan data.

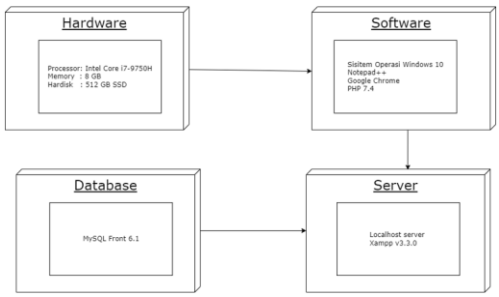
e. *Testing*
Pengujian sistem dilakukan untuk mengevaluasi kinerja dan keandalan aplikasi yang telah dibangun. Hasil dari seluruh tahapan pengujian ini akan menjadi dasar untuk analisis dan kesimpulan mengenai kelayakan sistem dalam mengamankan dokumen nasabah PT Asuransi Jiwa Astra. Tahapan pengujian ini berfokus pada tiga aspek utama:
1) *Black-box Testing*
Pengujian ini dilakukan untuk memastikan setiap fitur aplikasi (unggah, enkripsi, dekripsi, simpan, unduh) berfungsi sesuai dengan yang diharapkan.
2) *Performance Testing*
Mengukur kecepatan proses enkripsi dan dekripsi pada dokumen dengan berbagai ukuran (misal: 1MB, 2MB, 3MB).
3) *Security Testing*
Menguji mekanisme pengelolaan kunci untuk memastikan tidak ada

P ISSN : 2549-0710
E ISSN : 2722-2713

celah yang dapat dieksploitasi oleh pihak yang tidak berwenang.

HASIL DAN PEMBAHASAN

Untuk memastikan algoritma *Advanced Encryption Standard* (AES) dapat berjalan secara optimal, komponen perangkat lunak dan keras yang digunakan dalam penerapannya harus memenuhi persyaratan teknis tertentu. Gambar 2 menunjukkan komponen *software* yang dipakai adalah PC dengan Windows OS 10, *notepad++, google chrome* dan PHP 7.4; *hardware* yang digunakan adalah *processor intel core* i7-9750H dengan *memory* 8 GB dan *harddisk* SSD 512 GB; *database* yang dipakai menggunakan MySQL *Front* 6.1. kemudian ketiga hal yang disebutkan diatas akan menggunakan *localhost server* dengan hasil kompilasi menggunakan xampp v3.3.0.



Gambar 2. Spesifikasi *hardware* dan *software*

Upaya menjaga integritas dan pengamanan *file* dalam penelitian dilakukan dengan memanfaatkan algoritma kriptografi AES 128-bit. Tahapan implementasi algoritma pada *website* adalah sebagai berikut:

a. *Login*
Login sangat dibutuhkan pada proses saat masuk ke dalam suatu sistem, guna menjaga keamanan data dengan memasukkan identitas (Arieska & Mukti, 2023), untuk memberikan akses sesuai dengan identitas pengguna sistem tersebut.

Gambar 3. Tampilan layar *login*

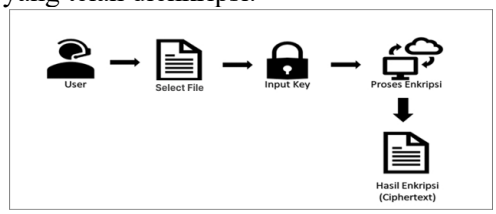
Gambar 3 adalah proses *login* yang harus dilakukan, dengan memasukkan, *username* dan *password,* jika kedua hal tersebut sesuai, akan tampil tampilan layar utama (*dashboard*).

Gambar 4. Tampilan layar utama

Gambar 4 merupakan tampilan layar utama dari akun *project manager*, dimana penggunanya dapat melakukan *activity* sebagai berikut:

1) *Button User*
Pengguna dapat melihat akun yang aktif dalam sistem.
2) *Button* Enkripsi
Pengguna dapat melihat banyaknya *file* yang sudah terenkripsi.
3) *Button* Dekripsi
Pengguna dapat melihat banyaknya *file* yang sudah terdekripsi.
4) Menu *File*
Pada menu ini, pengguna dapat melakukan proses enkripsi atau dekripsi.
5) Menu Daftar *List*
Berisikan daftar status file yang terenkripsi atau terdekripsi.
6) Menu Tentang
Pada menu ini, berisikan informasi singkat, tujuan dan fungsi sistem.
7) Menu Bantuan
Terdapat cara mengatasi masalah umum dan *Frequency Asked Question* (FAQ).

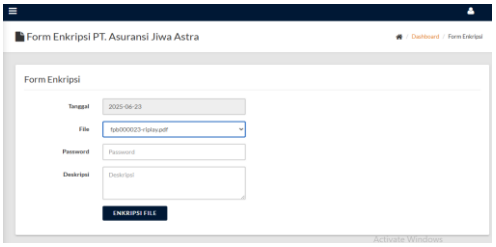
b. Enkripsi
Tahap ini menunjukkan proses enkripsi data serta menampilkan *output* dari data yang telah dienkripsi.



Gambar 5. Proses enkripsi

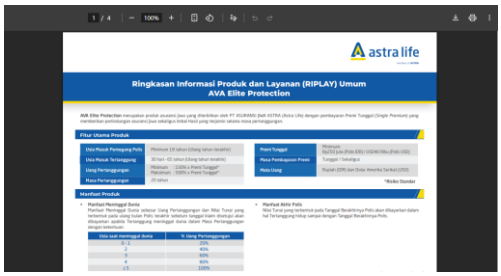
Gambar 5 menjelaskan proses enkripsi dimana admin akan memilih *file* asli dan *input key,* kemudian hasil enkripsi berupa *ciphertext* akan keluar jika proses enkripsi sudah berhasil dijalankan.

P ISSN : 2549-0710
E ISSN : 2722-2713

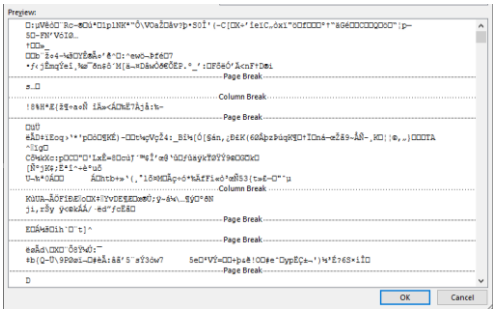


Gambar 6. Tampilan layar *form* enkripsi

Enkripsi *file* dapat dilakukan pada gambar 6, selain memilih *file* asli seperti gambar 7, admin juga harus memasukkan *password* dan dekripsi dari *file* tersebut. Setelah mengklik *button* "ENKRIPSI *FILE*" akan tampil *chipertext preview* seperti gambar 8.



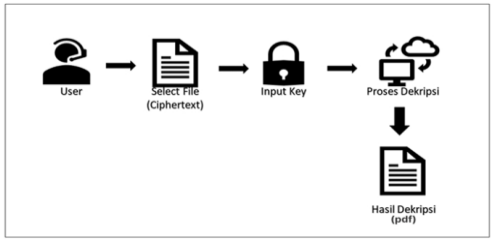
Gambar 7. *File* asli



Gambar 8. *Ciphertext preview*

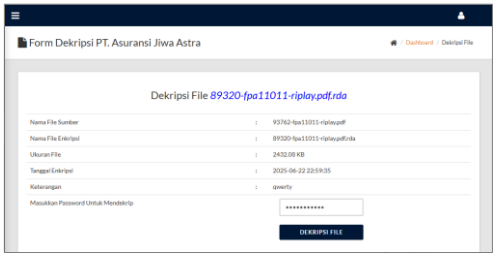
c. Dekripsi

Pada tahap ini diperlihatkan proses dekripsi data beserta hasil data yang telah berhasil didekripsi.



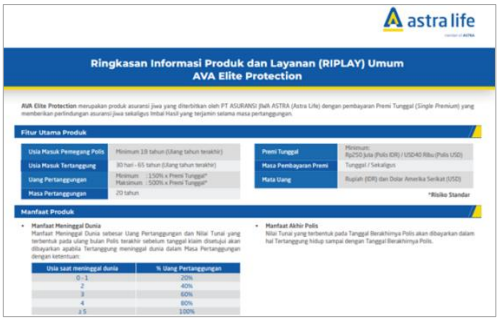
Gambar 9. Proses dekripsi

Gambar 9 merupakan proses dekripsi dimana admin akan memilih *file* yang sudah dienkripsi sebelumnya (*ciphertext*), dan *input key* yang sesuai, maka akan keluar hasilnya ketika proses dekripsi selesai.



Gambar 10. Tampilan layar *form* dekripsi

Proses dekripsi dapat dilakukan pada gambar 10, ketika admin telah memilih *file* yang sudah dienkripsi seperti gambar 8, admin diharuskan untuk memasukan *password* yang sama pada saat proses enkripsi. Jika *password* sesuai, maka proses dekripsi dapat dikatakan selesai dengan menghasilkan *output* seperti gambar 11.



Gambar 11. Hasil dekripsi

Pengujian pada tahap ini dilakukan untuk membandingkan proses enkripsi dan dekripsi terhadap *file* atau berkas. Tabel 1 dan 2 dilakukan pengujian dengan cara *black-box testing* untuk mendeteksi kesalahan yang mungkin terjadi, dari proses enkripsi dan dekripsi pada *website* yang dibuat, menyatakan bahwa proses dan hasil dari enkripsi dan dekripsi telah sesuai atau berjalan sesuai dengan fungsinya.

Tabel 1. *Black-box testing* menu enkripsi data

Pengujian	Harapan	Hasil
Enkripsi *file*	Data yang telah melalui proses enkripsi hanya dapat diakses dengan *password* yang *valid*, dan ukuran *file* tetap tidak mengalami perubahan.	Sesuai dengan harapan
Proses enkripsi	*File* hasil enkripsi tidak dapat diakses atau dibaca dalam bentuk aslinya.	Sesuai dengan harapan
Hasil	Memperlihatkan isi	Sesuai

Enkripsi	data dalam kondisi terenkripsi yang tidak dapat dikenali.	dengan harapan

Tabel 2. *Black-box testing* menu dekripsi data

Pengujian	Harapan	Hasil
Dekripsi *file*	Data yang telah di dekripsi bisa dibaca kembali dengan isi yang masih sama seperti semula.	Sesuai dengan harapan
Hasil dekripsi	Menampilkan text asli dari *file* tersebut.	Sesuai dengan harapan

Pengujian yang kedua adalah *performance testing* untuk memastikan bahwa *website* yang dibuat beroperasi sesuai dengan algoritma yang diterapkan. *Performance testing* dibagi menjadi 3 skenario, diantaranya: normal, batas dan ekstrem. *Performance testing* dengan skenario normal pada tabel 3 menghasilkan *performance* dari proses enkripsi dan dekripsi pada *website* dapat dijalankan dengan semestinya, dengan arti bahwa berkas asli yang sudah di enkripsi, dapat dikembalikan lagi keasliannya setelah melewati proses dekripsi dengan *password* atau *key* yang sesuai.

Tabel 3. *Performance testing* (skenario normal)

Skenario	*Input*	Hasil
Enkripsi *file* pdf	*File* .pdf ukuran 1 MB	*File* terenkripsi berhasil disimpan
Ciphertext	*File* .pdf ukuran 2 MB	*File* berhasil dienkripsi dan dapat didekripsi kembali dengan benar
Dekripsi *file* terenkripsi	*File* hasil enkripsi + kunci yang benar	*File* asli berhasil dikembalikan

Performance testing pada skenario batas pada tabel 4, membuktikan bahwa saat mengenkripsi berkas terjadi *error* jika pada proses enkripsi berkas yang dimasukkan adalah *file* dengan ukuran 0 KB dan terjadi pula *error* jika saat proses dekripsi dimasukkan *password* atau *key* yang tidak sesuai.

Tabel 4. *Performance testing* (skenario batas)

Skenario	*Input*	Hasil
Enkripsi *file* kosong	*File* .pdf ukuran 0 KB	Sistem menolak proses enkripsi dan menampilkan pesan *error*
Enkripsi *file* maksimum yang diperbolehkan	*File* .pdf ukuran 3 MB	*File* berhasil dienkripsi tanpa *crash*
Dekripsi dengan panjang kunci salah	*File* terenkripsi + kunci salah 1 karakter	Sistem menolak dekripsi dan menampilkan pesan *error*

Performance testing pada skenario ekstrem pada tabel 5, menjelaskan bahwa sistem yang dirancang tidak bisa mengenkripsi berkas atau *file* yang berukuran besar dan tidak bisa mengenkripsi *file* yang bukan menjadi standar pada sistem.

Tabel 5. *Performance testing* (skenario ekstrem)

Skenario	*Input*	Hasil
Enkripsi *file* sangat besar	*File* .pdf ukuran 1 GB	Sistem memproses atau menampilkan pesan bahwa ukuran melebihi kapasitas
Enkripsi *file* non-standar	*File* .exe, .iso	Sistem Menolak dan menampilkan pesan bahwa format tidak sesuai.

Hasil implementasi sistem aplikasi enkripsi dan dekripsi dokumen menggunakan algoritma *Advanced Encryption Standard* (AES) 128-bit menunjukkan bahwa seluruh fungsi utama aplikasi berjalan sesuai dengan rancangan. Uji fungsionalitas dilakukan terhadap fitur unggah, enkripsi, dekripsi, penyimpanan, dan unduh dokumen. Pengujian dilakukan pada 20 sampel *file* dengan ukuran bervariasi, maksimal 3 MB. Hasilnya, semua fitur berhasil dijalankan tanpa error, menghasilkan tingkat keberhasilan 100%. Pengujian performa menunjukkan bahwa proses enkripsi membutuhkan waktu rata-rata 3,35 detik untuk *file* berukuran 3 MB, sedangkan proses dekripsi membutuhkan waktu rata-rata 3,20 detik. Dari sisi keamanan, pengujian menggunakan simulasi menunjukkan tingkat efektivitas perlindungan mencapai 99%, sehingga *file* tidak dapat dibaca tanpa kunci yang *valid*.

Berdasarkan hasil pengujian, sistem aplikasi yang dibangun terbukti mampu memenuhi tiga aspek utama: fungsionalitas, performa, dan keamanan.

a. Fungsionalitas Sistem
   Seluruh fitur berjalan optimal sesuai kebutuhan pengguna. Integrasi antara proses unggah, enkripsi/dekripsi,

penyimpanan, dan unduh otomatis memastikan alur kerja yang efisien. Tingkat keberhasilan 100% pada uji fungsional menunjukkan stabilitas sistem yang tinggi.

b. Performa Aplikasi
Waktu eksekusi enkripsi dan dekripsi yang berkisar di bawah 4 detik untuk *file* hingga 3 MB tergolong cepat, sehingga dapat diterapkan pada operasional perusahaan tanpa mengganggu produktivitas. Efisiensi ini menunjukkan bahwa algoritma AES-128 dapat diimplementasikan pada sistem dengan sumber daya komputasi standar.

c. Keamanan Data
Tingkat efektivitas perlindungan mencapai 99% menunjukkan bahwa AES-128 mampu mencegah akses tidak sah secara signifikan. Hal ini sejalan dengan keunggulan AES sebagai algoritma yang telah direkomendasikan oleh NIST dan digunakan secara luas dalam industri dan memadai untuk melindungi dokumen rahasia.

KESIMPULAN

Merujuk pada hasil pelaksanaan dan pengujian sistem yang telah dilakukan, sistem kriptografi dengan metode AES-128 berhasil diterapkan untuk meningkatkan perlindungan terhadap data sensitif nasabah di PT Asuransi Jiwa Astra tanpa mengganggu proses yang sudah berjalan. Integrasi metode enkripsi ini ke dalam sistem manajemen dokumen elektronik berjalan dengan baik untuk seluruh fungsi utama seperti unggah, enkripsi, penyimpanan, dekripsi, dan unduh dokumen berjalan tanpa *error* dalam berbagai skenario uji (normal, batas, dan ekstrem), dengan tingkat keberhasilan 100%.

REFERENSI

Abdullah, R. K., Azhar, N. F., Mujahidin, S., & Hoan, R. O. (2025). Penerapan Enkripsi Hibrida AES-RSA Untuk Meningkatkan Keamanan Layanan Sistem Informasi Distribusi Slip Gaji. *Jambura Journal of Electrical and Electronics Engineering (JJEEE)*, *7*(1), 33–40. https://doi.org/https://doi.org/10.37905/jjeee.v7i1.28737

Arieska, A. E. B., & Mukti, F. S. (2023). Pemanfaatan One-Time Password dan Algoritma Advanced Encryption Standard dalam Sistem Login Internet Kampus. *G-Tech: Jurnal Teknologi Terapan*, *7*(4), 1262–1271. https://doi.org/https://doi.org/10.33379/gtech.v7i4.3003

Baqis, A. M., & Nasution, M. I. P. (2025). Pentingnya Perlindungan dan Keamanan Data Privasi di Era Digital. *Jurnal Manajemen dan Pendidikan Agama Islam*, *3*(3), 396–404. https://doi.org/https://doi.org/10.61132/jmpai.v3i3.1150

Bhagaskara, G. P. K., & Priyanto, I. M. D. (2024). Perlindungan Hukum terhadap Nasabah Terkait Bocornya Data Nasabah Berdasarkan Perspektif Hukum Perbankan. *Eksekusi : Jurnal Ilmu Hukum dan Administrasi Negara*, *2*(2), 162–170. https://doi.org/10.55606/eksekusi.v2i2.1099

Butarbutar, R. (2023). Kejahatan Siber Terhadap Individu : Jenis , Analisis , dan Perkembangannya. *Technology and Economics Law Journal Volume*, *2*(2), 299–317. https://doi.org/https://doi.org/10.21143/TELJ.vol2.no2.1043

Handayani, I. P., & Pradana, R. (2023). Smart Home Controlling Menggunakan PLC Method. *Jurnal TICOM (Technoology of Information and Computer)*, *11*(2), 108–112. https://doi.org/https://doi.org/10.70309/ticom.v11i2.79

Handoyo, E., Kriswantoro, M. C., & Anugrah, B. (2025). Analisis Keamanan Siber Kampus Menggunakan Framework Cobit 2019 Pada Domain Delivery, Service and Support (DSS). *JIKA (Jurnal Informatika)*, *9*(2), 159–168. https://doi.org/https://10.31000/jika.v9i2.12845

Hasibuan, E. S., & Putri, E. A. (2024). Perlindungan Keamanan Atas Data Pribadi Di Dunia Maya. *Jurnal Hukum Sasana*, *10*(1), 70–83. https://doi.org/https://doi.org/10.31599/sasana.v10i1.2134

Ihtisyamuddin, A., Hartanto, F., & Kurniawan, E. D. (2024). Penyalahgunaan Teknologi Komputer untuk Tindakan Kriminal Siber dalam Novel Simvlacrm Karya Cassandra & Noorca Marendra Massardi. *Jupiter: Publikasi Ilmu Keteknikan Industri, Teknik Elektro dan Informatika*, *2*(1), 179–189. https://doi.org/https://doi.org/10.61132/jupiter.v2i1.68

Mediana. (2024). Kemenkominfo Tangani 111 Kasus Kebocoran Data Pribadi Sepanjang 2019-2024. *kompas.id*, 1. https://www.kompas.id/artikel/111-kasus-kebocoran-data-pribadi-ditangani-kemenkominfo-pada-2019-14-mei-2024

Nanda, N. A., Silalahi, S. M. S., Fatricia Nasution, D., Sari, M., & Gunawan, I. (2023). Kriptografi dan Penerapannya Dalam Sistem Keamanan Data. *Jurnal Media Informatika*, *4*(2), 90–93. https://doi.org/10.55338/jumin.v4i2.428

Nopriadi, N. (2024). Menjaga Privasi Digital: Studi Tentang Kesadaran Mahasiswa dalam Perlindungan Data Pribadi di Media Sosial. *Polygon : Jurnal Ilmu Komputer dan Ilmu Pengetahuan Alam*, *2*(6), 87–97. https://doi.org/https://doi.org/10.62383/polygon.v2i6.297

Nugraha, D. A., Nurfitroh, R., Ul-Haq, N. D., Dika, R. P., & Lagontang, S. N. (2025). Kebocoran Data BPJS Kesehatan: Ancaman Terhadap Keamanan Informasi Publik di Era Digital. *Integrative Perspectives of Social and Science Journal (IPSSJ)*, *2*(3), 4685–4691. https://economy.okezone.com/read/2021/05/25/320/2415107/kebocoran-data-bpjs-kesehatan-dirut-karena-peretasan

Ramadhan, A. A. I., Rivanti, E. Z., & Zulva, R. S. (2023). Implementasi Kriptografi AES Menggunakan Bahasa Java Programming: Meningkatkan Keamanan Data Melalui Enkripsi & Dekripsi Yang Kuat. *Jurnal Pendidikan Teknologi Informasi*, *2*(1), 20–26. https://jurnal.umj.ac.id/index.php/TripleA/article/view/17513%0Ahttps://jurnal.umj.ac.id/index.php/TripleA/article/download/17513/9646

Rizky, P. A., Soim, S., & Sholihin. (2024). Implementasi Algoritma Kriptografi AES CBC Untuk Keamanan Komunikasi Data Pada Hardware. *RESISTOR (Rekayasa Sistem Komputer)*, *7*(2), 71–78. https://doi.org/https://doi.org/10.31598/jurnalresistor.v7i2.1650

Saripa, S. (2024). Implementasi Sistem Keamanan File Menggunakan Algoritma AES untuk Mengamankan File Pribadi. *Progressive Information, Security, Computer, and Embedded System (PISCES)*, *1*(2), 138–148. https://doi.org/https://doi.org/10.61255/pisces.v1i2.100

Suari, K. R. A., & Sarjana, I. M. (2023). Menjaga Privasi di Era Digital: Perlindungan Data Pribadi di Indonesia. *Jurnal Analisis Hukum*, *6*(1), 132–146. https://doi.org/https://doi.org/10.38043/jah.v6i1.4484

Sulung, U., & Muspawi, M. (2024). MEMAHAMI SUMBER DATA PENELITIAN: PRIMER, SEKUNDER, DAN TERSIER. *Edu Research*, *5*(3), 110–116. https://doi.org/https://doi.org/10.47827/jer.v5i3.238

Wachid Hidayatulloh, N., Tahir, M., Amalia, H., Afdlolul Basyar, N., Faizal Prianggara, A., & Yasin, M. (2023). Mengenal Advance Encrytion Standard (AES) Sebagai Algoritma Kriptografi Dalam Mengamankan Data. *Digital Transformation Technology (Digitech)*, *03*(1), 1–10. https://doi.org/https://doi.org/10.47709/digitech.v3i1.2293