SENAFTI
SEMINAR NASIONAL MAHASISWA
FAKULTAS TEKNOLOGI INFORMASI

6th Seminar Nasional Mahasiswa Fakultas Teknologi Informasi (SENAFTI)
20 September 2025 – Jakarta, Indonesia
Volume 4, Nomor 2, September 2025 - ISSN 2962-8628 (*online*)

PERBANDINGAN ALGORITMA KRIPTOGRAFI AES-128 DAN DES UNTUK KEAMANAN DOKUMEN PADA PT JASA RAHARJA PUTERA

Sultan Nabil[1*], Hari Soetanto[2]

[1,2] Teknik Informatika, Fakultas Teknologi Informasi, Universitas Budi Luhur, Kota Tangerang, Indonesia

Email: [1*]sultannabil110@gmail.com, [2]hari.soetanto@budiluhur.ac.id
(* : corresponding author)

Abstrak- PT Jasa Raharja Putera menghadapi masalah keamanan pada dokumen digital rahasia yang rentan terhadap kebocoran data ketika berpindah perangkat atau dikirim melalui jaringan. Permasalahan ini semakin kompleks karena metode pengamanan tradisional, seperti proteksi *password* bawaan aplikasi, tidak cukup kuat menahan serangan modern. Oleh karena itu, diperlukan pendekatan kriptografi dengan algoritma yang terbukti mampu melindungi data sensitif. Penelitian ini mengembangkan aplikasi berbasis *web* dengan metode enkripsi dan dekripsi menggunakan algoritma kriptografi simetris *Advanced Encryption Standard* 128-bit (AES-128) dan *Data Encryption Standard* (DES). Perbandingan kedua algoritma dipilih karena AES-128 dikenal lebih modern dan efisien, sementara DES masih banyak digunakan secara historis meskipun keamanannya telah dipertanyakan. Sistem dibangun menggunakan bahasa pemrograman *PHP* dengan basis data *MySQL*, serta mendukung dua peran pengguna, yaitu *admin* dan *user*, dengan hak akses yang berbeda. Metode pengujian dilakukan dengan menyiapkan *file* uji dari berbagai format umum (PDF, DOCX, PPTX, XLSX, dan PNG) dan ukuran bervariasi. Setiap *file* diproses melalui enkripsi dan dekripsi menggunakan kedua algoritma untuk mengukur beberapa parameter, yaitu waktu eksekusi, perubahan ukuran file, serta akurasi hasil dekripsi. Hasil penelitian menunjukkan bahwa AES-128 memiliki kinerja lebih baik dibandingkan DES, terutama dari sisi kecepatan enkripsi dan dekripsi pada semua *file* uji. Selain itu, kedua algoritma menghasilkan ukuran *file* terenkripsi yang hampir sama dengan *file* asli, sehingga efisiensi penyimpanan tetap terjaga. Proses dekripsi berhasil mengembalikan *file* ke bentuk semula tanpa kerusakan. Temuan ini mempertegas bahwa AES-128 lebih layak digunakan untuk kebutuhan keamanan dokumen modern, sedangkan DES dapat dijadikan pembanding historis namun kurang efisien untuk implementasi praktis. Aplikasi yang dirancang terbukti mampu meningkatkan perlindungan dokumen digital secara fungsional dan dapat dijadikan acuan bagi pengembangan sistem keamanan serupa pada perusahaan maupun instansi lain.

Kata Kunci: Kriptografi, AES-128, DES, Enkripsi, Dekripsi, Keamanan data

Comparison of AES-128 and DES Encryption Algorithms for Document Security at PT Jasa Raharja Putera

Abstract- *In corporate environments such as PT Jasa Raharja Putera, the management of confidential and sensitive digital documents is highly vulnerable to data breaches, particularly during file transfers between devices or when transmitted over networks without adequate protection. Such risks pose a significant challenge, as potential unauthorized access may compromise the confidentiality and integrity of internal company information. This study proposes the design and implementation of a web-based application to secure documents through encryption and decryption using two symmetric cryptographic algorithms: Advanced Encryption Standard 128-bit (AES-128) and Data Encryption Standard (DES). The application was developed using PHP with a MySQL database and supports two distinct user roles administrator and regular user with clearly defined access privileges. Performance evaluation was conducted on various common file formats, including PDF, DOCX, PPTX, XLSX, and PNG, measuring encryption–decryption processing time, file size variations, and decryption accuracy. The testing involved processing files of different sizes with both algorithms to compare their performance. Experimental results indicate that AES-128 consistently outperforms DES in terms of execution speed across all tested file types, while preserving file integrity and compatibility without corruption after decryption. The developed system can be effectively utilized by both user roles, meeting corporate document security requirements efficiently. These findings provide a practical reference for the development of robust, web-based document security solutions applicable not only to corporate settings but also to other organizations requiring strong data protection measures.*

Keywords*: cryptography, AES-128, DES, encryption, decryption, data security*

1. PENDAHULUAN

Perkembangan teknologi informasi yang semakin pesat memberikan kemudahan dalam pengelolaan, penyimpanan, dan distribusi data. Namun, kemajuan ini juga menimbulkan tantangan serius terkait keamanan informasi, terutama dalam menghadapi ancaman kebocoran data yang dapat berdampak pada kerugian finansial, reputasi, maupun kepercayaan publik terhadap suatu institusi. Data yang bersifat sensitif, seperti dokumen internal perusahaan, membutuhkan perlindungan yang memadai agar kerahasiaan, integritas, dan ketersediaannya tetap terjaga [1].

Salah satu solusi yang umum digunakan dalam menjaga keamanan data adalah kriptografi. Kriptografi modern menyediakan berbagai algoritma enkripsi yang dirancang untuk mengamankan data dari akses pihak yang tidak berwenang. *Advanced Encryption Standard* (AES) merupakan salah satu algoritma kriptografi yang banyak digunakan karena memiliki tingkat keamanan yang tinggi, efisiensi proses, serta kemampuan dalam menangani berbagai ukuran data. AES-128, khususnya, menawarkan keseimbangan yang baik antara keamanan dan performa [1]. Di sisi lain, algoritma *Data Encryption Standard* (DES) meskipun lebih sederhana dan telah digunakan sejak lama, saat ini mulai ditinggalkan karena tingkat keamanannya yang relatif rendah terhadap serangan *brute force* [2].

Beberapa penelitian sebelumnya menunjukkan fokus yang berbeda terkait penerapan algoritma kriptografi. [3] meneliti implementasi AES untuk pengamanan dokumen, terutama dalam konteks file teks dan dokumen keuangan, namun penelitian tersebut tidak menampilkan perbandingan langsung dengan algoritma lain. Di sisi lain, [4] melakukan kajian terhadap blok *cipher* DES yang menekankan kelemahan algoritma tersebut dalam menghadapi serangan modern, tetapi belum membandingkan secara praktis dengan algoritma yang lebih kuat seperti AES pada konteks aplikasi berbasis *web*. Penelitian [5] justru mengkaji perbandingan kinerja enkripsi antara AES dan RC4, sehingga arah pembahasan lebih menekankan perbedaan algoritma lain dan tidak memberikan gambaran khusus mengenai AES-128 dan DES.

Selain itu, tinjauan internasional yang dilakukan oleh [6] menegaskan bahwa AES memiliki tingkat keamanan dan efisiensi yang lebih baik dibandingkan DES, tetapi pembahasan mereka hanya bersifat konseptual tanpa implementasi spesifik pada aplikasi pengelolaan dokumen. Dari berbagai studi tersebut terlihat bahwa masih terdapat celah penelitian, yaitu kurangnya kajian praktis yang membandingkan AES-128 dan DES secara langsung dalam konteks sistem pengelolaan dokumen berbasis *web*. Oleh karena itu, penelitian ini hadir untuk mengisi kekosongan tersebut dengan melakukan implementasi sekaligus analisis perbandingan performa kedua algoritma dalam lingkungan aplikasi nyata.

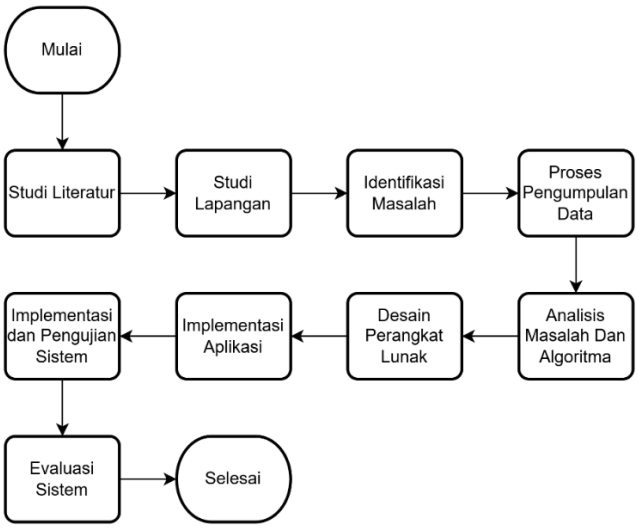
Penelitian ini dibatasi pada implementasi dan analisis algoritma kriptografi AES-128 dengan kunci 128-bit dan DES dengan kunci 64-bit (56-bit efektif dan blok 64-bit) pada aplikasi berbasis *web* yang difokuskan untuk proses enkripsi dan dekripsi dokumen. Ukuran *file* yang dapat dienkripsi dibatasi maksimal 8MB guna menjaga performa aplikasi selama pengujian, dengan format file yang didukung meliputi *.doc, .docx, .txt, .pdf, .xls, .xlsx, .ppt, .pptx, .jpg, .jpeg, .png, .gif, .mp3, .mp4, .mov,* dan *.mpg*. Aspek perbandingan yang dianalisis terbatas pada kecepatan proses enkripsi dan dekripsi serta ukuran file hasil enkripsi dan dekripsi.

Tujuan penelitian ini adalah merancang dan mengimplementasikan aplikasi pengamanan dokumen berbasis *web* dengan metode enkripsi dan deskripsi menggunakan AES-128 dan DES, sekaligus melakukan analisis perbandingan performa keduanya pada dokumen internal PT Jasa Raharja Putera. Aspek yang dianalisis mencakup kecepatan proses, ukuran *file* hasil enkripsi, dan akurasi dekripsi, dengan harapan dapat memberikan rekomendasi algoritma yang paling optimal bagi perusahaan serta menjadi referensi pengembangan sistem keamanan informasi di masa depan.

2. METODE PENELITIAN

2.1 Tahapan Metode

Pengembangan sistem pada penelitian ini dilakukan secara terstruktur dengan menyesuaikan kebutuhan di PT Jasa Raharja Putera. Setiap tahap saling terhubung, mulai dari pengumpulan informasi, pemilihan algoritma, implementasi sistem, hingga evaluasi hasil perbandingan AES-128 dan DES. Tahapan metode dapat dilihat pada Gambar 1. dibawah.



Gambar 1. Tahapan Metode

2.1.1 Studi Literatur

Pada tahap ini dilakukan penelusuran pustaka dari jurnal, buku, dan penelitian terdahulu yang berkaitan dengan kriptografi simetris, khususnya algoritma AES-128 dan DES. Literatur yang dikaji meliputi kelebihan, kelemahan, serta hasil uji performa pada berbagai konteks, sehingga diperoleh dasar teori untuk membandingkan kedua algoritma dalam penelitian ini.

2.1.2 Studi Lapangan

Observasi dilakukan di PT Jasa Raharja Putera untuk memahami kondisi nyata pengelolaan dokumen internal. Ditemukan bahwa dokumen digital perusahaan sering berpindah antarperangkat dan dikirim melalui jaringan, sehingga berisiko mengalami kebocoran data. Informasi dari studi lapangan ini menjadi landasan perumusan kebutuhan sistem.

2.1.3 Identifikasi Masalah

Berdasarkan studi literatur dan studi lapangan, diidentifikasi permasalahan utama, yaitu lemahnya metode perlindungan dokumen yang hanya mengandalkan password bawaan aplikasi. Hal ini menimbulkan kebutuhan akan sistem berbasis kriptografi yang mampu menjaga kerahasiaan dokumen internal.

2.1.4 Proses Pengumpuan Data

Data yang dikumpulkan berupa sampel *file* dengan format umum (PDF, DOCX, PPTX, XLSX, dan PNG) yang digunakan untuk pengujian sistem. *File* dipilih dengan ukuran bervariasi, mulai dari kecil hingga mendekati 8 MB, sesuai dengan batas maksimum yang ditetapkan pada aplikasi.

2.1.5 Analisis Masalah Dan Algoritma

Pada tahap ini dilakukan pemilihan algoritma yang akan dibandingkan, yaitu AES-128 dan DES. Analisis difokuskan pada parameter performa meliputi:

a. Waktu eksekusi proses enkripsi dan dekripsi.
b. Perubahan ukuran *file* setelah dienkripsi.
c. Keakuratan hasil dekripsi (integritas *file*).

2.1.6 Desain Perangkat Lunak

Rancangan sistem dibuat dalam bentuk arsitektur aplikasi *web* berbasis PHP dengan *database MySQL*. Desain mencakup *class diagram*, rancangan basis data, serta alur proses enkripsi-dekripsi. Sistem dirancang memiliki dua peran pengguna, yaitu *admin* (mengelola *user* & dokumen) dan *user* (mengunggah, mengenkripsi, dan mendekripsi dokumen).

2.1.7 Implementasi Aplikasi

Tahap ini mewujudkan rancangan sistem menjadi aplikasi *web* yang dapat dijalankan. Implementasi mencakup pembuatan halaman *login*, *dashboard*, enkripsi-dekripsi (AES-128 dan DES), daftar dokumen, manajemen pengguna, serta halaman informasi Perusahan.

2.1.8 Implementasi dan Pengujian Sistem

Sistem diuji menggunakan metode *blackbox testing* pada setiap *fitur* (*login*, enkripsi, dekripsi, manajemen dokumen, dan pengguna). Selain itu, dilakukan pengujian kinerja algoritma dengan menjalankan proses enkripsi-dekripsi pada sampel *file* dari berbagai ukuran dan format, sehingga diperoleh data perbandingan performa antara AES-128 dan DES.

2.1.9 Evaluasi Sistem

Evaluasi dilakukan berdasarkan hasil pengujian performa. Parameter yang dievaluasi meliputi kecepatan proses, perubahan ukuran file, serta akurasi hasil dekripsi. Hasil evaluasi digunakan untuk menarik kesimpulan mengenai algoritma yang paling sesuai diterapkan pada pengelolaan dokumen internal di PT Jasa Raharja Putera.

2.2 Kriptografi

Kriptografi berasal dari bahasa Yunani *kryptos* (tersembunyi) dan *graphein* (menulis), merupakan disiplin ilmu yang mempelajari teknik pengamanan komunikasi dan informasi melalui kode [7]. Tujuannya adalah memastikan data hanya dapat diakses pihak berwenang serta menjaga integritas dan keasliannya selama transmisi atau penyimpanan [8].

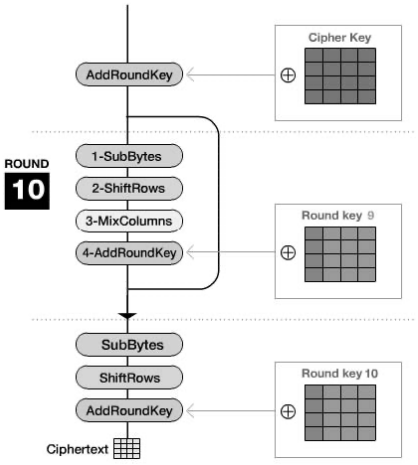
2.3 *Advanced Encryption Standard* (AES)

AES adalah algoritma kriptografi simetris jenis *block cipher* yang dipilih oleh NIST pada tahun 2001 untuk menggantikan DES yang sudah tidak aman terhadap serangan modern [9]. AES berbasis algoritma Rijndael karya Joan Daemen dan Vincent Rijmen, dan menjadi standar enkripsi global di berbagai sektor.
Karakteristik utama AES [10], [11]:

a. *Block cipher* simetris, menggunakan kunci yang sama untuk enkripsi dan dekripsi.
b. Ukuran blok tetap 128 bit.
c. Panjang kunci 128, 192, atau 256 bit (penelitian ini fokus pada AES-128).
d. Jumlah putaran: 10 (AES-128), 12 (AES-192), 14 (AES-256).
e. Operasi berbasis *byte*.
f. Data direpresentasikan sebagai matriks 4x4 *byte* (*State*).

2.4 *Proses Enkripsi AES-128*

Enkripsi AES-128 adalah proses mengubah blok data *plaintext* 128-bit menjadi *ciphertext* 128-bit melalui 10 ronde transformasi.



Gambar 2. Proses Enkripsi AES
(Sumber: https://www.researchgate.net/figure/Gambar-3-Diagram-Proses-Enkripsi_fig4_315812818)

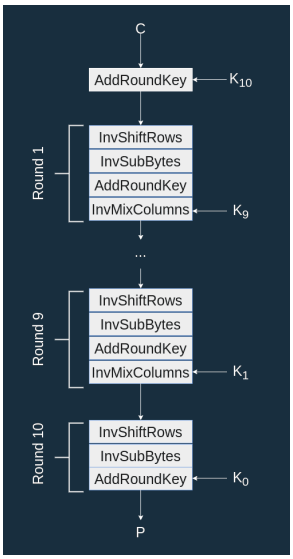
2.5 Contoh Perhitungan Proses Enkripsi AES-128

Untuk menunjukkan mekanisme, berikut contoh ringkas enkripsi kata "sultannabil" (11 karakter, diproses sebagai 128-bit blok ASCII dengan padding).

a. *Plaintext* (ASCII → Hex)**:**
   73 75 6C 74 61 6E 6E 61 62 69 6C 00 00 00 00 00.
   (*padding* nol untuk memenuhi 16 *byte*/128 bit).
b. Kunci (contoh 128-bit):
   2B 7E 15 16 28 AE D2 A6 AB F7 97 75 46 20 63 5A.
c. Langkah awal (*AddRoundKey*):
   73 XOR 2B = 58, 75 XOR 7E = 0B, … (dilakukan untuk 16 *byte*).
d. *SubBytes*: setiap byte diganti via S-Box, misalnya 58 → 8A, 0B → 77, dst.
e. *ShiftRows*: baris kedua digeser 1 *byte*, baris ketiga 2 *byte*, baris keempat 3 *byte*.
f. *MixColumns*: setiap kolom dimultiplikasi matriks *Galois Field* GF(2^8).
g. *AddRoundKey* (akhir ronde 10): menghasilkan *ciphertext* akhir.
h. *Ciphertext* (hasil akhir, *hex*):
   8A F3 4C 92 6D 2B 01 B7 C1 45 6E 29 73 90 5D E8.
i. *Ciphertext* (dalam base64):
   ivNMk m0rAbfBRW4pc5Bd6A==

2.6 Proses Dekripsi AES-128

Dekripsi AES-128 merupakan kebalikan dari proses enkripsi, menggunakan transformasi *invers* untuk mengembalikan *ciphertext* menjadi *plaintext* secara akurat [13]. Ilustrasi lengkap alur proses dapat dilihat pada gambar 3.



Gambar 3. Proses Dekripsi AES-128
(Sumber: https://translate.google.com/translate?u=https://braincoke.fr/blog/2020/08/the-aes-decryption-algorithm-explained/&hl=id&sl=en&tl=id&client=imgs)

Tahapan proses dekripsi AES-128:

a. *InvShiftRows*: Menggeser baris matriks *State* ke kanan secara siklik dengan *offset* sesuai *ShiftRows*, namun arah berlawanan.
b. *InvSubBytes*: Menggantikan setiap *byte* pada *State* menggunakan *Inverse S-Box* untuk membalik substitusi saat enkripsi.
c. *InvMixColumns*: Mengalikan setiap kolom *State* dengan matriks *invers* di medan *Galois* GF(2^8) untuk membalik efek *MixColumns*.

d. *AddRoundKey*: Melakukan operasi XOR antara *State* dan *round key* yang sesuai. Pada tahap awal dekripsi, langkah ini membalik efek *AddRoundKey* pada enkripsi, dan pada ronde terakhir menghasilkan *plaintext* semula.

2.7 *Data encryption Standart (DES)*

DES adalah algoritma kriptografi simetris yang dikembangkan oleh IBM dan disahkan sebagai standar enkripsi oleh NIST pada tahun 1977. Algoritma ini menggunakan panjang kunci 56-bit untuk mengenkripsi blok data 64-bit. Meskipun kini dianggap kurang aman terhadap serangan *brute-force* modern, DES memiliki nilai historis penting karena menjadi dasar pengembangan algoritma seperti 3DES dan AES [14].

2.8 Contoh Proses Enkripsi DES-64

Proses enkripsi DES mengubah plaintext 64-bit menjadi ciphertext 64-bit melalui 16 putaran jaringan *Feistel*. Setiap putaran menggunakan satu subkunci yang dihasilkan dari kunci asli melalui proses *key schedule*. Urutan langkah enkripsi sebagai berikut [14]. Sebagai ilustrasi, kata "sultan nabil" (11 karakter) diubah ke ASCII lalu dipotong 8 *byte* pertama sebagai 64-bit *plaintext*

a. *Plaintext* (ASCII → Hex, 8 *byte*):
   "sultan n" → 73 75 6C 74 61 6E 20 6E.
b. Kunci (contoh 64-bit, efektif 56-bit):
   13 34 57 79 9B BC DF F1
c. *Initial Permutation* (IP)**:** bit *plaintext* dipermutasi, misalnya 73 (01010011) berubah posisi bit-nya sesuai tabel IP.
d. Pembagian blok. L1 = R0, R1 = L0 ⊕ F(R0, K1)
e. Setelah 16 ronde + Swap + FP diperoleh hasil akhir.
f. *Ciphertext* (hex):
   85 E8 13 54 0F 0A B4 05.
g. *Ciphertext* (base64):
   hegTVA8KtAU=

2.9 Proses Dekripsi DES-64

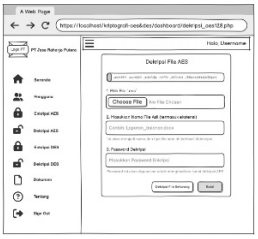
Dekripsi DES bekerja dengan prinsip yang sama seperti enkripsi karena sifat simetris jaringan Feistel. Perbedaannya hanya pada urutan penggunaan subkunci yang dibalik, dari *K16* hingga *K1* [14] . Berikut langkah-langkah dekripsi DES:

a. *Initial Permutation* (IP): Melakukan permutasi awal pada *ciphertext*.
b. Pembagian Blok Data: Memisahkan hasil IP menjadi *L0* dan *R0* masing-masing 32-bit.
c. 16 Putaran Feistel: Sama seperti enkripsi, tetapi subkunci digunakan terbalik.
d. Pertukaran (Swap): Menukar blok hasil putaran ke-16.
e. *Final Permutation* (FP): Menghasilkan *plaintext* asli.

2.10 *Rancangan Layar*

Pada penelitian ini, rancangan layar difokuskan pada bagian inti aplikasi, yaitu proses enkripsi dan dekripsi pada algoritma AES-128 dan DES, karena bagian inilah yang menjadi fokus utama pengembangan sistem. Rancangan dapat dilihat pada gambar 4,5,6 & 7 dibawah.

Gambar 4. Rancangan layar enkripsi AES-128



Gambar 5. Rancangan layar dekripsi AES-128

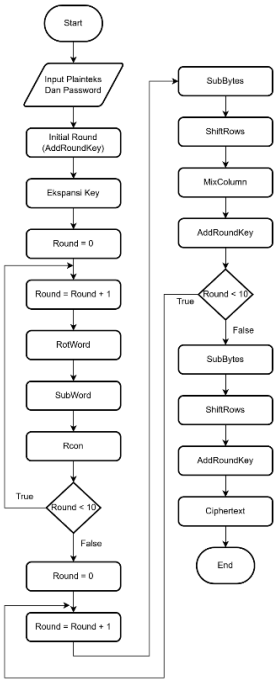
Gambar 6. Rancangan layar enkripsi DES

Gambar 7. Rancangan layar dekripsi DES

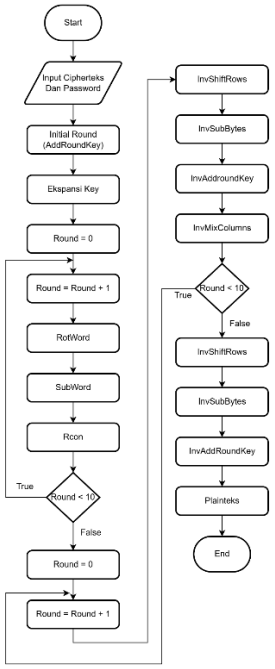
3. HASIL DAN PEMBAHASAN

3.1 *Flowchart*

Dalam penelitian ini, *flowchart* digunakan untuk memvisualisasikan alur kerja proses enkripsi dan dekripsi AES-128 secara sistematis. Pada proses enkripsi, langkah dimulai dari *input plainteks* dan kunci, kemudian dilakukan proses ekspansi kunci untuk menghasilkan *round key*, diikuti transformasi bertahap seperti *SubBytes, ShiftRows, MixColumns,* dan *AddRoundKey* hingga menghasilkan *ciphertext*. Sementara itu, proses dekripsi merupakan kebalikan dari enkripsi, dimulai dari input *ciphertext* dan kunci, lalu melewati tahapan *invers* seperti *InvShiftRows, InvSubBytes, InvMixColumns*, serta *AddRoundKey* untuk mengembalikan *ciphertext* menjadi *plaintext* semula. *Flowchart* dapat dilihat pada gambar 8 & 9 berikut ini.



Gambar 8. *Flowchart* Proses Enkripsi AES-128



Gambar 9. *Flowchart* Proses Dekripsi AES-128

3.2 Spesifikasi Sistem

Spesifikasi sistem mencakup lingkungan pengembangan, bahasa pemrograman, basis data, serta perangkat keras yang digunakan dalam proses pembuatan dan pengujian aplikasi. Detail spesifikasi ditunjukkan pada plainteks semula.

Tabel 1. Lingkungan Pengembangan

Kategori	Spesifikasi	**Keterangan**
Lingkungan Pengembangan	XAMPP v3.3.0	Paket *server* lokal yang digunakan untuk pengembangan.
	Apache 2.4.54 (Win64)	*Web server* untuk menangani permintaan HTTP.
	PHP 7.4.33	Bahasa pemrograman utama di sisi *server*.

Bahasa & Teknologi	MariaDB/MySQL	Sistem manajemen *database*.
	PHP	Logika utama aplikasi (enkripsi, dekripsi, manajemen *file*).
	HTML	Struktur halaman *web*.
	CSS	*Styling* dan *layout* antarmuka pengguna.
	JavaScript	Interaksi dinamis di sisi klien (misalnya, toggle menu).
	SQL	Bahasa untuk berkomunikasi dengan *database*.
Database	MariaDB/MySQL	Digunakan untuk menyimpan data pengguna dan metadata *file*.
Perangkat Keras (Pengujian)	Prosesor: Intel® Core™ i7-9750H Memori: 8 GB DDR4 RAM Penyimpanan: 512 GB SSD Sistem Operasi: Windows 11	Spesifikasi mesin yang digunakan untuk pengembangan dan pengujian kinerja.

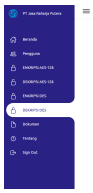
3.3 Tampilan Layar

Tampilan layar berikut menunjukkan hasil implementasi antarmuka pengguna pada halaman proses enkripsi dan dekripsi menggunakan algoritma AES-128 dan DES. Setiap halaman dirancang agar pengguna dapat dengan mudah memilih file, memasukkan kunci, dan menjalankan proses enkripsi atau dekripsi. Tampilan dapat dilihat pada gambar 10,11,12, & 13 dibawah.

Gambar 10. Tampilan layar proses enkripsi AES-128

Gambar 11. Tampilan layar proses dekripsi AES-128

Gambar 12. Tampilan layar proses enkripsi DES



Gambar 13. Tampilan layar proses dekripsi DES

3.4 Hasil Perbandingan

Pengujian dilakukan untuk membandingkan kinerja algoritma AES-128 dan DES pada proses enkripsi dan dekripsi pada berbagai jenis file. Parameter yang diukur meliputi ukuran file sebelum dan sesudah enkripsi, ukuran hasil dekripsi, serta waktu yang dibutuhkan untuk proses enkripsi dan dekripsi. Pengujian dilakukan pada beberapa format file seperti PDF, PPTX, XLSX, DOCX, dan PNG untuk melihat pengaruh tipe dan ukuran file terhadap performa kedua algoritma.

Tabel 2. Perbandingan Hasil Enkripsi & Dekripsi

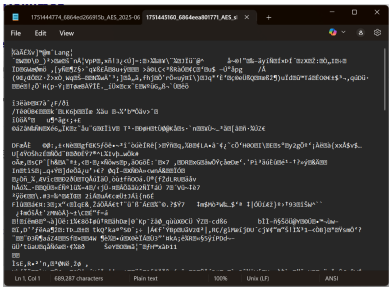
No	Nama File	Format	Ukuran Asli (KB)	Algoritma	Ukuran Enkripsi (KB)	Ukuran Dekripsi (KB)	Waktu Enkripsi (detik)	Waktu Dekripsi (detik)
1	Annual Report 2024 PT Jasa Raharja Putera (Short Version).pdf	pdf	3338.00 KB	AES-128	3337.11 KB	3338.00 KB	21.29 Detik	49.29 Detik
				DES	3337.10 KB	3338.00 KB	66.56 Detik	76.72 Detik
2	Sosialisasi Pajak Daerah	pptx	673.12 KB	AES-128	673.14 KB	673.12 KB	4.30 Detik	8.72 Detik
				DES	673.13 KB	673.12 KB	13.00 Detik	13.41 Detik
3	Data_Klaim_Jasa_Raharja_Putera	xlsx	13.95 KB	AES-128	13.97 KB	13.95 KB	0.09 Mili Detik	0.19 Mili Detik
				DES	13.96 KB	13.95 KB	0.31 Mili Detik	0.28 Mili Detik

4	profil-asuransi-pt-jasa-raharja-putera	docx	55.55 KB	AES-128	55.56 KB	55.55 KB	0.36 Mili Detik	0.74 Mili Detik
				DES	55.55 KB	55.55 KB	1.10 Detik	1.11 Detik
5	Logo_JRP_Insurance	png	180.31 KB	AES-128	180.33 KB	180.31 KB	1.12 Detik	2.41 Detik
				DES	180.32 KB	180.31 KB	3.65 Detik	3.49 Detik

3.5 Hasil Proses Enkripsi dan Dekripsi

Subbab ini menampilkan hasil keluaran dari aplikasi setelah melakukan proses enkripsi dan dekripsi menggunakan algoritma AES-128 atau DES. Setiap *screenshot* berisi hasil perubahan yang terjadi pada file sebelum dan sesudah proses. Tampilan ini sekaligus menjadi bukti bahwa algoritma berhasil diimplementasikan sesuai fungsi yang diharapkan. Tampilan di tunjukkan pada gambar 14,15, & 16.

Gambar 14. Tampilan File Sebelum Dienkripsi



Gambar 15. Tampilan File Sesudah enkripsi AES-128

Gambar 16. Tampilan File Sesudah enkripsi DES

3.6 Analisis Hasil

Berdasarkan Tabel 2, terlihat bahwa ukuran *file* hasil enkripsi maupun dekripsi dari kedua algoritma hampir sama dengan ukuran asli, dengan selisih yang sangat kecil (0,01–0,02 KB). Hal ini menunjukkan bahwa baik AES-128 maupun DES tidak menambah *overhead* signifikan terhadap ukuran *file*, sehingga keduanya efisien dalam penggunaan ruang penyimpanan. Namun, perbedaan paling mencolok muncul pada parameter waktu eksekusi. Misalnya, pada *file Annual* Report 2024.pdf berukuran 3.338 KB, proses enkripsi menggunakan AES-128 hanya membutuhkan 21,29 detik, sementara DES memerlukan 66,56 detik. Pola yang sama terlihat di semua format *file* lain: pada Sosialisasi Pajak Daerah.pptx, AES-128 memerlukan 4,30 detik, sedangkan DES mencapai 13 detik. Bahkan untuk *file* kecil seperti Data Klaim.xlsx, AES-128 selesai dalam 0,09 milidetik, sementara DES tetap lebih lambat di 0,31 milidetik. Angka-angka ini mengindikasikan konsistensi keunggulan AES-128 dari sisi performa waktu dibandingkan DES, baik pada file besar maupun kecil.

Perbedaan kecepatan ini dapat dijelaskan dari sisi kompleksitas algoritmik. AES-128 dirancang dengan struktur *Substitution-Permutation Network (SPN)* yang lebih efisien, menggunakan operasi substitusi *byte*, pergeseran baris, pencampuran kolom, dan penambahan kunci. Operasi ini berbasis aritmatika sederhana (*byte-level*) yang dapat diproses paralel, sehingga menurunkan waktu eksekusi. Sebaliknya, DES menggunakan arsitektur *Feistel network* dengan 16 putaran yang melibatkan fungsi-fungsi bit-*level* lebih rumit, termasuk permutasi awal dan akhir serta ekspansi kunci 56-bit. Kompleksitas *bitwise* ini menyebabkan *overhead* komputasi yang lebih tinggi, terutama ketika ukuran *file* semakin besar. Dengan demikian, perbedaan struktur internal kedua algoritma inilah yang menjadi penyebab utama AES-128 selalu lebih cepat dibandingkan DES dalam pengujian ini.

4. KESIMPULAN

Berdasarkan hasil penelitian, aplikasi keamanan dokumen berbasis *web* dengan penerapan algoritma kriptografi AES-128 dan DES berhasil dikembangkan dan berfungsi sesuai tujuan. Sistem mampu melakukan proses enkripsi dan dekripsi pada berbagai jenis *file* digital secara efisien. Hasil pengujian menunjukkan bahwa AES-128 memiliki kinerja lebih unggul dibandingkan DES, terutama dalam kecepatan proses, meskipun keduanya menghasilkan ukuran *file* terenkripsi yang hampir sama. Penerapan sistem ini dapat meningkatkan perlindungan dokumen digital dari ancaman pencurian data atau akses tidak sah.

Peneliti mengucapkan terima kasih kepada PT Jasa Raharja Putera atas dukungan dan fasilitas yang diberikan selama proses penelitian ini berlangsung.

DAFTAR PUSTAKA

[1] Y. R. Setiawan dan S. Mulyati, "Implementasi Kriptografi Algoritme Advanced Encryption Standard (Aes-128) Untuk Pengamanan Dokumen Berbasis Web Pada Pt . Xyz," vol. 3, no. April, hal. 30–39, 2024.

[2] M. Pradesh dan M. Pradesh, "Comparative Study of Various Parameters of Des and AES Encryption Schemes," vol. 44, no. 7, hal. 2511–2518, 2023.

[3] M. Azhari, D. I. Mulyana, F. J. Perwitosari, dan F. Ali, "Implementasi Pengamanan Data pada Dokumen Menggunakan Algoritma Kriptografi Advanced Encryption Standard (AES)," *J. Pendidik. Sains dan Komput.*, vol. 2, no. 01, hal. 163–171, 2022, doi: 10.47709/jpsk.v2i01.1390.

[4] R. Munir, "Review Beberapa Block Cipher DES," hal. 1–34, 2021.

[5] F. K. Wardhana, A. Kurniawan, B. R. Seto, dan I. A. Saputro, "Analisis Perbandingan Kinerja Enkripsi Algoritma RC4 Dan AES," *Pros. Semin. Nas. AMIKOM SURAKARTA 2023*, no. November, hal. 124–134, 2023.

[6] M. N. Alenezi, H. Alabdulrazzaq, dan N. Q. Mohammad, "Symmetric encryption algorithms: Review and evaluation study," *Int. J. Commun. Networks Inf. Secur.*, vol. 12, no. 2, hal. 256–272, 2020.

[7] A. R. Harahap dan T. A. Salim, "Sistem Kriptografi pada Pengamanan Autentikasi Dokumen Elektronik: Systematic Literature Review," *Khazanah J. Pengemb. Kearsipan*, vol. 16, no. 2, hal. 203, 2023, doi: 10.22146/khazanah.81893.

[8] R. Rahman *et al.*, "Peningkatan Keamanan Data dengan Kriptografi Modern pada Sistem Operasi," no. 4, hal. 2–9, 2024.

[9] S. Oktaviani, F. Rizky, dan I. Gunawan, "Analisis Keamanan Data Dengan Menggunakan Kriptografi Modern Algoritma Advance Encryption Standar (AES)," *J. Media Inform.*, vol. 4, no. 2, hal. 97–101, 2023, doi: 10.55338/jumin.v4i2.435.

[10] K. A. Mckay dan D. A. Cooper, "Withdrawn NIST Technical Series Publication," no. 2001, hal. 27–28, 2019.

[11] N. Wachid Hidayatulloh, M. Tahir, H. Amalia, N. Afdlolul Basyar, A. Faizal Prianggara, dan M. Yasin, "Mengenal Advance Encrytion Standard (AES) Sebagai Algoritma Kriptografi Dalam Mengamankan Data," *Digit. Transform. Technol.*, vol. Vol.03, no. No.1, hal. 1–10, 2023, [Daring]. Tersedia pada: https://jurnal.itscience.org/index.php/digitech/article/view/2293

[12] Melenia Bayu Aryanto, Muhlis Tahir, Silvia Irma Devita, Zuda Nuril Mustofa, Qurrotun Ainiyah, dan Shelviatus Sundoro, "Implementasi Enkrip Dan Dekrip File Menggunakan Metode Advance Encryption Standard (AES-128)," *J. Ilm. Sist. Inf. dan Ilmu Komput.*, vol. 3, no. 1, hal. 89–104, 2023, doi: 10.55606/juisik.v3i1.434.

[13] D. E. Fitriani, N. Zulatifa, D. P. Anggraini, I. Ady, dan S. Indonesia, "Analisis Implementasi Enkripsi Dan Dekripsi Menggunakan Algoritma Advanced Encryption Standard
(AES) PADA JAVA," no. November, hal. 57–67, 2024.

[14] B. Alnur, Mulyono, Fitri Amillia, dan S. Sutoyo, "JITE (Journal of Informatics andTelecommunication Engineering)," *J. Informatics Telecommun. Eng.*, vol. 7, no. 1, hal. 102–111, 2023, [Daring]. Tersedia pada: https://www.researchgate.net/publication/335117624_Malang_City_Polytechnic_Web_Based_Student_Attendance_Information_System_Telecommunications_Engineering_Study_Program_Using_Fingerprint/fulltext/5d515fe34585153e594ef214/Malang-City-Polytechnic-Web-Based-S