INOVATE : Jurnal Ilmiah Inovasi Teknologi Informasi **e-ISSN : 2654-3788**
Penerbit: Fakultas Teknologi Informasi Universitas Hasyim Asy'ari **p-ISSN:2654-3788**
Vol. , No. B, September 2025 (pp-pp). **DOI: 10.33752/inovate.v10i1.9251**

ANALISIS TINGKAT KEAMANAN FILE DOKUMEN MENGGUNAKAN ALGORITMA ADVANCED ENCRYPTION STANDARD (AES)

Hasan Shadzily[1)]; Bambang Sujatmiko[2)]
[1,2)] Fakultas Teknologi Informasi, Universitas Hasyim Asy'ari Jombang Jawa Timur Indonesia
hasan@mhs.unhasy.ac.id[1], bsujatmiko@unhasy.ac.id[2]

Abstrak

Keamanan data pada file dokumen yang dikirim atau disimpan secara digital merupakan salah satu permasalahan di era teknologi saat ini. Terutama penggunaan platform digital untuk berbagi informasi dapat menjadi sasaran pencurian data, maka dibutuhkan solusi untuk melindungi kerahasiaan dan integritas data yang dikirimkan melalui jaringan internet. Salah satu cara yang dapat mengatasi permasalah ini adalah dengan menerapkan algoritma kriptografi yang aman dan mudah di implementasikan, salah satunya adalah Advanced Encryption Standard (AES) dengan panjang kunci 128 bit. AES merupakan algoritma yang telah terbukti keamanannya dan banyak digunakan untuk melindungi data dalam berbagai aplikasi. Dengan mengenkripsi file dokumen menggunakan AES, data yang dikirimkan melalui platform digital dapat terlindungi kerahasiannya dan mencegah akses dari pihak yang tidak sah, karena hanyak pihak yang memiliki kunci yang dapat mendekripsinya. Hasil uji keacakan ciphertext menggunakan shannon entropy didapatkan nilai entropy rata-rata sebesar 7.96. Nilai tersebut membuktikan bahwa tingkat keacakan dari ciphertext sangat tinggi, mendekati nilai maksimal 8 yang menghasilkan ciphertext yang acak, sehingga memperkuat keamanan data dari potensi analisis pola atau serangan kriptanalis.

Kata Kunci: file dokumen, AES, keamanan data, enkripsi, dekripsi.

DOCUMENT FILE SECURITY LEVEL ANALYSIS USING ADVANCED ENCRYPTION STANDARD (AES) ALGORITHM

Abstract

Data security in document files that are sent or stored digitally is one of the problems in the current technological era. Especially the use of digital platforms to share information can be a target for data theft, so a solution is needed to protect the confidentiality and integrity of data sent over the internet network. One way to solve this problem is to implement a secure and easy-to-implement cryptographic algorithm, one of which is the Advanced Encryption Standard (AES) with a key length of 128 bits. AES is an algorithm that has proven its security and is widely used to protect data in various applications. By encrypting document files using AES, data sent via digital platforms can be protected and prevent access from unauthorized parties, because only those who have the key can decrypt it. The results of the ciphertext randomness test using Shannon entropy obtained an average entropy value of 7.96. This value proves that the randomness level of the ciphertext is very high, approaching the maximum value of 8 which produces a random ciphertext, thus strengthening data security from potential pattern analysis or cryptanalyst attacks.

eywords: document files, AES, data security, encryption, decryption.

1. PENDAHULUAN

Pengaruh perkembangan teknologi saat ini memudahkan manusia saling bertukar data dan informasi secara digital (Fitria D dkk., 2022). Namun, informasi yang dipertukarkan baik melalui jaringan internet atau platform digital memiliki risiko terhadap pencurian data (Eka Putri dkk., 2021). Apabila data penting tersebut bocor, maka dapat mengancam kerahasiaannya dan memberikan peluang bagi pihak yang yang tidak berwenang untuk menyebarluaskan data tersebut yang tentunya dapat mengakibatkan kerugian besar bagi individu atau organisasi yang bersangkutan (Shita dan Hin, 2021). Oleh karena itu, dibutuhkan suatu metode yang menjadi solusi dalam melindungi data maupun informasi yang disimpan atau dikirimkan melalui platform digital agar aman dari akses pihak yang tidak berwenang.

Kriptografi merupakan suatu teknik yang digunakan untuk melindungi keamanan data dan mengutamakan aspek baik dari kerahasiaan, integritas data, otentikasi, dan anti penyangkalan (Eka Putri dkk., 2021). Secara umum, cara kerja

kriptografi yaitu mengubah data asli (plaintext) menjadi data rahasia (ciphertext) yang tidak dapat dibaca (Simamarta dkk., 2019). Advanced Encryption Standard (AES) sebagai standar algoritma kriptografi simetris terkini yang memiliki kemampuan untuk menjawab tantangan teknologi komunikasi yang berkembang sangat cepat serta keunggulannya dalam keamanan, kecepatan, dan tentunya mudah diimplementasikan. AES juga mampu mengenkripsi data dengan panjang kunci mulai dari 128 bit, 192 bit, dan 256 bit (Muttaqin dan Rahmadoni, 2020). Hal ini tentunya sangat cocok untuk digunakan dalam aplikasi yang membutuhkan sistem dengan tingkat keamanan yang tinggi.

Melalui penelitian ini, diharapkan dapat menghasilkan sebuah aplikasi yang dapat melakukan enkripsi maupun dekripsi data dengan mengimplementasikan algoritma AES, serta memberikan kontribusi yang signifikan dalam memperkuat pemahaman tentang efektivitas dan efesiensi algoritma AES ECB dalam menjaga keamanan data.

2. METODE PENELITIAN

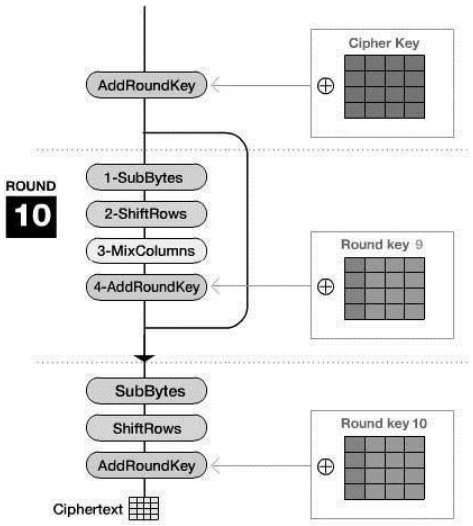
2.1 Advanced Encryption Standard (AES)

Algoritma AES adalah sebuah algoritma kriptografi simetris berbasis cipher block yang menggunakan kunci yang identik untuk proses enkripsi dan dekripsi. Selain itu, input dan output berupa blok dengan ukuran bit yang telah ditentukan (Shita dan Hin, 2021). AES dapat melakukan enkripsi dan dekripsi pada blok data sebesar 128 bit dengan menggunakan panjang kunci yang bervariasi mulai dari 128 bit, 192 bit, dan 256 bit (Simamarta dkk., 2019). Panjang kunci yang digunakan akan mempengaruhi jumlah round (Nr) yang digunakan pada masing-masing panjang kunci yang dapat dilihat pada Tabel 1.

Tabel 1. Jumlah Round dan Panjang Kunci (Setiawan & Mufarrihah, 2024)

Tipe	Panjang Kunci (Nk Words)	Panjang Blok (Nb words)	Jumlah Round (Nr)
AES-128	4	4	10
AES-192	6	4	12
AES-256	8	4	14

Bagaimana algoritma AES Rijndael beroperasi pada blok 128 bit dengan kunci 128 bit. Berikut adalah ilustrasi cara kerja dari algoritma AES yang ditunjukan pada Gambar 1.



Gambar 1. Algoritma AES-128 bit (Shita & Hin, 2021)

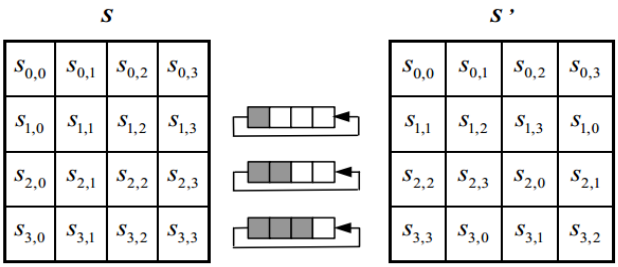
Pada Gambar 1. Dilakukan round sebanyak 10 putaran dengan melalui empat operasi utama yaitu (Muttaqin dan Rahmadoni, 2020):

1. AddRoundKey
   Pada tahap AddRoundkey dilakukan penggabungan antara state dengan round key menggunakan operasi XOR.
2. SubBytes
   Pada tahap SubByte dilakukan subtitusi setiap byte dengan nilai yang diambil dari tabel subtitusi (S-Box).

x \ y	0	1	2	3	4	5	6	7	8	9	a	b	c	d	e	f
0	63	7c	77	7b	f2	6b	6f	c5	30	01	67	2b	fe	d7	ab	76
1	ca	82	c9	7d	fa	59	47	f0	ad	d4	a2	af	9c	a4	72	c0
2	b7	fd	93	26	36	3f	f7	cc	34	a5	e5	f1	71	d8	31	15
3	04	c7	23	c3	18	96	05	9a	07	12	80	e2	eb	27	b2	75
4	09	83	2c	1a	1b	6e	5a	a0	52	3b	d6	b3	29	e3	2f	84
5	53	d1	00	ed	20	fc	b1	5b	6a	cb	be	39	4a	4c	58	cf
6	d0	ef	aa	fb	43	4d	33	85	45	f9	02	7f	50	3c	9f	a8
7	51	a3	40	8f	92	9d	38	f5	bc	b6	da	21	10	ff	f3	d2
8	cd	0c	13	ec	5f	97	44	17	c4	a7	7e	3d	64	5d	19	73
9	60	81	4f	dc	22	2a	90	88	46	ee	b8	14	de	5e	0b	db
a	e0	32	3a	0a	49	06	24	5c	c2	d3	ac	62	91	95	e4	79
b	e7	c8	37	6d	8d	d5	4e	a9	6c	56	f4	ea	65	7a	ae	08
c	ba	78	25	2e	1c	a6	b4	c6	e8	dd	74	1f	4b	bd	8b	8a
d	70	3e	b5	66	48	03	f6	0e	61	35	57	b9	86	c1	1d	9e
e	e1	f8	98	11	69	d9	8e	94	9b	1e	87	e9	ce	55	28	df
f	8c	a1	89	0d	bf	e6	42	68	41	99	2d	0f	b0	54	bb	16

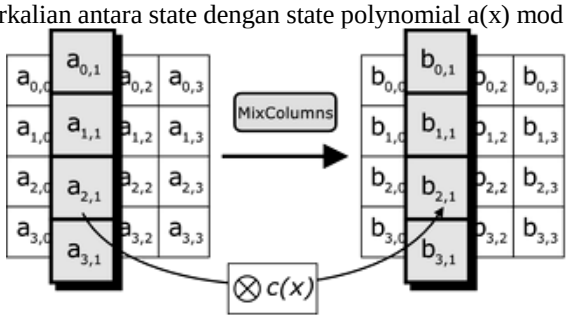
Gambar 2. Tabel S-Box

3. ShiftRows
Pada tahap ini dilakukan proses pergeseran byte dimana byte paling kiri akan digeser ke kiri secara sirkuler.



Gambar 3. ShiftRows

4. MixColumn
Pada tahap ini dilakukan perkalian antara state dengan state polynomial a(x) mod (x4 + 1).



Gambar 4. MixColumn

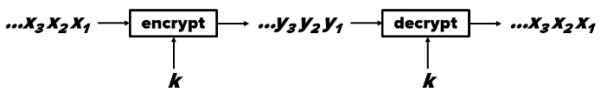
2.2 Electronic Codebook (ECB)

Electronic Codebook (ECB) adalah mode operasi yang digunakan pada algoritma kriptografi simetris berbasis cipher block yang setiap karakteristik blok plaintext yang identik akan menghasilkan blok ciphertext yang sama. Secara sistematis, enkripsi dengan mode ECB dinyatakan sebagai:

$$Y_i = e(X_i) \quad (1)$$

Sedangkan dekripsi dinyatakan sebagai:

$$X_i = e^{-1}(Y_i) = e^{-1}(e(X_i)) \quad (2)$$



Gambar 5. Mode Electronic Codebook (ECB) (Bujari dan Aribas, 2017)

Salah satu keuntungan menggunakan mode ECB yaitu sinkronisasi blok tidak diperlukan: penerima dapat mendekripsi blok yang diterima tanpa perlu mendekripsikan semuanya. Selain itu, kesalahan bit yang terkait dengan

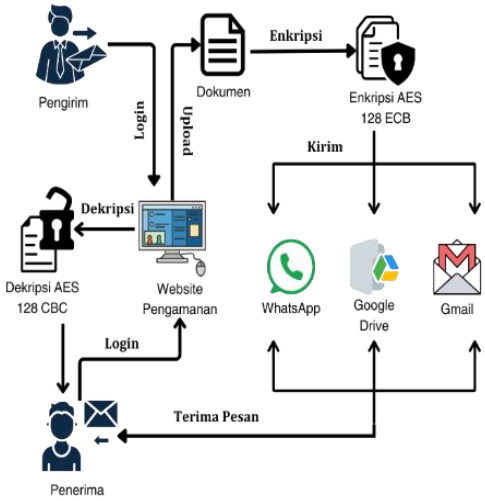
e-ISSN : 2654-3788
p-ISSN:2654-3788
DOI: 10.33752/inovate.v10i1.9251

beberapa kesalahan transmisi hanya berdampak pada blok terkait. Selain itu, penggunaan mode ECB dianggap cukup cepat, yang berasal dari kemampuan parelelisasi. Dengan kata lain, blok data yang berbeda dapat di enkripsi oleh unit enkripsi yang berbeda secara parallel. Karena kecepatan dan keunggulan paralelisasi, mode ini telah digunakan dalam berbagai aplikasi keamanan (Bujari dan Aribas, 2017).

3. HASIL DAN PEMBAHASAN

3.1 Rancangan Sistem

Dalam perancangan ini, sistem yang akan dibangun adalah sistem yang mampu melakukan enkripsi dan dekripsi pada file dokumen. Sistem ini menerapkan algoritma AES dan dibangun menggunakan bahasa pemrograman PHP. Sistem akan di implementasikan dalam bentuk website. Adapun untuk struktur sistem yang akan dibuat dapat dilihat pada Gambar 6. arsitektur sistem.



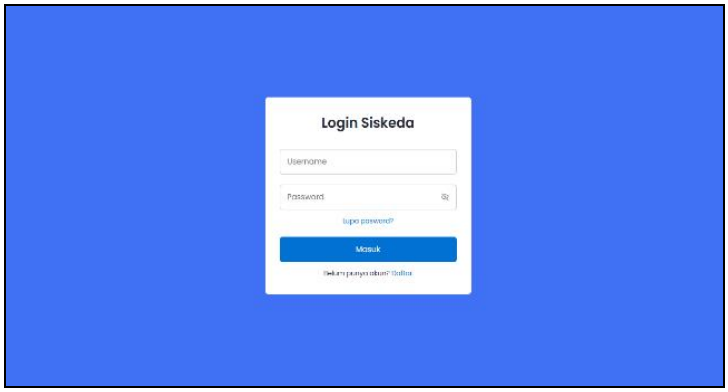
Gambar 6. Arsitektur Sistem

Pada Gambar 6. diuraikan dengan jelas arsitektur sistem yang akan dirancang mempunyai beberapa proses yaitu prose login pada halaman website, proses mengunggah file yang akan dienkripsi dan didekripsi, proses enkripsi, proses dekripsi, proses penyimpanan dan pengiriman file dokumen. Pada sistem yang akan dibangun proses enkripsi dan dekripsi menggunakan algoritma AES dengan panjang kunci 128 bit dan menggunakan mode operasi *Electronic Codebook* (ECB).

3.2 Interface Sistem

Hasil implementasi pada aplikasi sistem keamanan data menggunakan algoritma AES dengan tampilan antar muka sebagai berikut:

1. Tampilan Login
   Berikut ini adalah tampilan layar dari halaman login yang ditunjukan pada Gambar 7. terdapat input username dan password sebagai proses otentikasi. Jika input valid, pengguna akan dapat mengakses fitur yang ada pada aplikasi sistem seperti halaman enkripsi file dan halaman dekripsi file.

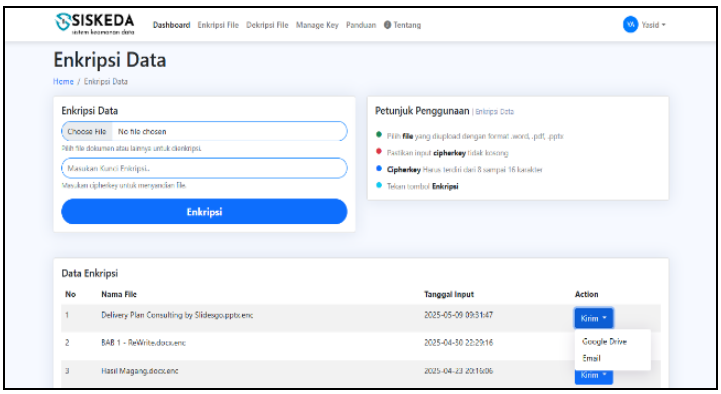


Gambar 7. Tampilan Login

2. Tampilan halaman enkripsi
   Halaman enkripsi digunakan untuk mengubah file dokumen yang dapat dibaca menjadi tidak dapat dibaca. Langkah untuk mengenkripsi file, pertama perlu memilih menu enkripsi file pada bagian navbar, selanjutnya

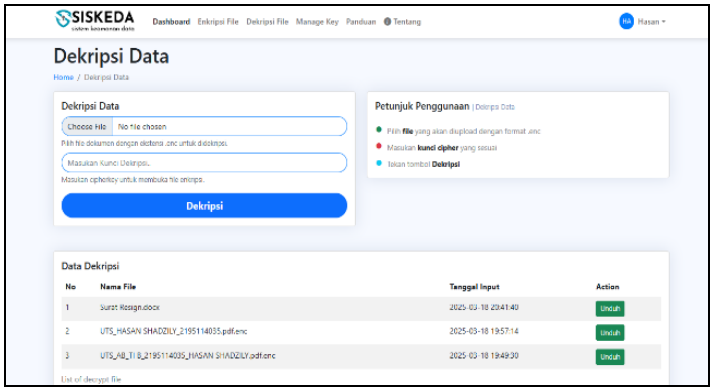
e-ISSN : 2654-3788
p-ISSN:2654-3788
DOI: 10.33752/inovate.v10i1.9251

pengguna memilih file yang akan dienkripsi dengan ketentuan data berupa text dan memasukan kunci enkripsi dengan panjang maksimal 16 karakter, file akan di enkripsi dengan menekan tombol enkripsi dan diproses menggunakan algoritma enkripsi AES-128-ECB.



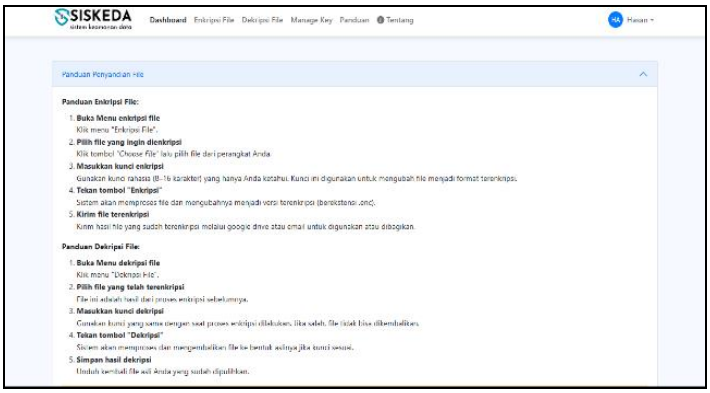
Gambar 8. Tampilan Halaman Enkripsi

3. Tampilan halaman dekripsi
Halaman dekripsi digunakan untuk mengembalikan dari bentuk file terenkripsi menjadi bentuk file semula yang dapat dibaca. Cara mendekripsi file, pengguna memilih menu dekripsi, kemudian pilih file yang akan di dekripsi dengan ketentuan format file yaitu .enc dan memasukan kunci yang sama ketika enkripsi file, sistem akan menjalankan proses dekripsi menggunakan algoritma dekripsi AES-128-ECB.



Gambar 9. Tampilan Halaman Dekripsi

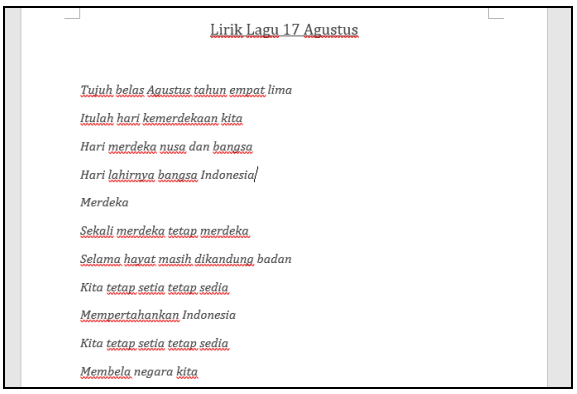
4. Tampilan halaman panduan
Halaman ini digunakan untuk memuat informasi tentang bagaimana penggunaan ataupun tata cara enkripsi dan dekripsi file pada aplikasi sistem ini. Berikut adalah tampilan halaman panduan yang ditunjukan pada Gambar 10.



Gambar 10. Tampilan Halaman Panduan Enkripsi dan Dekripsi

3.3 Hasil Enkripsi

Proses enkripsi melibatkan proses transformasi file asli (plaintext) menjadi file yang terenkripsi (ciphertext) yang isinya tidak dapat diakses atau dipahami tanpa proses dekripsi dan kunci yang tepat. Berikut adalah contoh dari file yang akan di enkripsi dan hasil file setelah di enkripsi.


Lirik Lagu 17 Agustus

Tujuh belas Agustus tahun empat lima
Itulah hari kemerdekaan kita
Hari merdeka nusa dan bangsa
Hari lahirnya bangsa Indonesia
Merdeka
Sekali merdeka tetap merdeka
Selama hayat masih dikandung badan
Kita tetap setia tetap sedia
Mempertahankan Indonesia
Kita tetap setia tetap sedia
Membela negara kita

Gambar 11. File Asli


Ln 1, Col 1 13.487 characters 100% Unix (LF) ANSI

Gambar 12. Hasil Enkripsi dari File Asli

Dapat dilihat pada Gambar 12. yang menunjukan bahwa hasil enkripsi dari file asli menghasilkan karakter-karakter yang acak dan tidak dapat dibaca maupun dipahami isinya.

3.4 Pengujian keamanan

Dilakukan uji keamanan dengan mengukur tingkat keacakan dari hasil enkripsi file menggunakan perhitungan shannon entropy. Perhitungan entropi dihitung menggunakan persamaan berikut :

$$H(x) = -\sum_{i=0}^{n} P(i)\ log_2(P(i)) \qquad (3)$$

Dimana X merupakan ciphertext yang akan dihitung keacakannya, P(i) untuk peluang munculnya i, dan i merupakan banyaknya kemunculan simbol. Jika hasil perhitungan shannon entropy menunjukan nilai entropy mendekati 8.00, berarti enkripsi berhasil menyamarkan pola ciphertext. Untuk data hasil pengujian shannon entropy ditunjukan pada Tabel 2.

Tabel 2. Hasil Pengujian Shannon Entropy

Nama File Terenkripsi	Nilai Entropy	Keterangan
Kalender Akademik 2024-2025 UNHASY.pdf.enc	7.9999	Tingkat keacakan tinggi
MAKALAH.docx.enc	7.9977	Tingkat keacakan tinggi
Data DPA Angkatan 2024 FTI.xlsx.enc	7.9886	Tingkat keacakan tinggi
Text.docx.enc	7.9854	Tingkat keacakan tinggi
No Hp, Email Dosen FTI.xlsx.enc	7.9940	Tingkat keacakan tinggi
FORM-Pendaftaran Seminar Proposal Dan Skripsi.doc.enc	7.8415	Tingkat keacakan tinggi
FORM-PI-FTI.doc.enc	7.9207	Tingkat keacakan tinggi
Logo Unhasy.docx.enc	7.9982	Tingkat keacakan tinggi

Dari hasil perhitungan uji pada Tabel 2. hasil perhitungan shannon entropy menunjukan bahwa rata-rata file memiliki nilai entropy sebesar 7.9657 yang mendekati nilai maksimalnya yaitu 8.00. Hal ini membuktikan bahwa

ciphertext memiliki tingkat keacakan yang tinggi, sehingga dapat memperkuat keamanan data dari potensi analisis pola dan serangan kriptanalis.

3.5 Pengujian kinerja

Dilakukan uji kinerja dengan mengukur waktu eksekusi pada proses enkripsi dan dekripsi. Hasil uji kecepatan enkripsi dan dekripsi dapat dilihat pada tabel 3. berikut :

Tabel 3. Hasil Uji Kecepatan Enkripsi dan Dekripsi

Nama File	Jenis Dokumen	Ukuran File	Waktu		Perangkat
			Enkripsi	Dekripsi	
Logounhasy.docx	Gambar	196 KB	0,0124 s	0,0051 ms	Laptop (Intel i5-10210U, 8GB RAM)
Logounhasy.docx	Gambar	196 KB	0,0057 s	0,0095 ms	Laptop (Intel i5-8250U, 8GB RAM)
Makalah.docx	Text + Gambar	185 KB	0,008 s	0,004 ms	Laptop (Intel i5-10210U, 8GB RAM)
Makalah.docx	Text + Gambar	185 KB	0,0281 s	0,0091 ms	Laptop (Intel i5-8250U, 8GB RAM)
Text.docx	Text	56 KB	0,0074 s	0,0317 ms	Laptop (Intel i5-10210U, 8GB RAM)
Text.docx	Text	56 KB	0,0234 s	0,0211 ms	Laptop (Intel i5-8250U, 8GB RAM)
Kecepatan rata-rata:			0,0092 s	0,0136 ms	Laptop (Intel i5-10210U, 8GB RAM)
			0,0190 s	0,0132 ms	Laptop (Intel i5-8250U, 8GB RAM)

Berdasarkan Tabel 3. dapat dilihat untuk uji coba kecepatan enkripsi dan dekripsi pada file dengan jenis dokumen dengan kategori yaitu gambar saja, text saja, atau gabungan gambar dan text, yang diuji menggunakan dua perangkat dengan spesifikasi berbeda. Hasil pengujian membuktikan bahwa algoritma AES mampu melakukan proses enkripsi dan dekripsi dalam waktu yang sangat singkat. Namun, kecepatan enkripsi dan dekripsi pada file hasilnya tidak selalu sama tergantung dengan hardware yang dipakai.

3.6 Evaluasi Program

Setelah dilakukan pengujian keamanan dan kinerja program pada sistem aplikasi ini, diperoleh kelebihan dan kekurangan dari aplikasi ini, sebagai berikut :

1. Memberikan sistem keamanan file yang aman dan efisien untuk digunakan.
2. Dapat melindungi file dari akses oleh pihak yang tidak berwenang.
3. Sistem memiliki tampilan yang sederhana dan mudah digunakan oleh pengguna.
4. File yang telah terenkripsi, menampilkan isi file dengan karakter acak yang tidak dapat dipahami.
5. Kecepatan yang dibutuhkan untuk proses enkripsi dan dekripsi sangat cepat.
6. Hasil enkripsi dan dekripsi dapat disimpan maupun dikirim melalui platform digital.

Kekurangan sistem:

1. Data yang digunakan tidak boleh berulang seperti dokumen berformat tetap karena pola pada ciphertext yang dihasilkan dari plaintext yang berulang dapat membuka peluang bagi penyerang untuk menganalisis struktur isi data.

4. KESIMPULAN

Berdasarkan hasil analisa terhadap permasalahan dan sistem yang dirancang, maka dapat diambil kesimpulan sebagai berikut:

1. Perancangan aplikasi dengan mengimplementasikan algoritma AES dapat memberikan solusi efektif untuk menjaga kerahasiaan isi dokumen. Sistem ini mampu mengenkripsi dan mendekripsi file dokumen dengan aman dan efisien yang telah dibuktikan melalui uji keamanan dan uji kinerja, sehingga dapat melindungi data dari akses yang tidak sah dan menjaga kerahasiaan informasi.
2. Implementasi algoritma AES dalam komunikasi digital dapat meningkatkan tingkat keamanan data yang dikirim dengan menyembunyikan isi informasi yang asli. Hal ini memastikan bahwa informasi yang dikirimkan tetap terlindungi dari ancaman penyadapan, sehingga memberikan rasa aman bagi pengguna dalam bertukar informasi secara digital

DAFTAR PUSTAKA

Bujari, D. & Aribas, E., 2017. *Comparative Analysis of Block Cipher Modes of Operation*, Istanbul: International Advanced Researches & Engineering Congress-2017.

D, N. I., Putri, N., & Zahrani, P. (2022). Literature Review Determinasi Infrastruktur Ti: Telekomunikasi, Internet Dan Brainware. *Jurnal Manajemen Pendidikan dan Ilmu Sosial*, *III*(2), 561-572.

Muttaqin, K., & Rahmadoni, J. (2020). Analysis And Design Of File Security System Aes (Advanced Encryption Standard) Cryptography Based. *Journal of Applied Engineering and Technological Science*, *I*(2), 113-123.

Putri, A. E., Kartikadewi, A., & Rosyid, L. A. (2020). Implementasi Kriptografi Dengan Algoritma Advanced Encryption Standard (Aes) 128 Bit Dan Steganografi Menggunakan Metode End Of File (Eof) Berbasis Java Desktop Pada Dinas Pendidikan Kabupaten Tangerang. *Applied Information Systems And Management (Aism), 2*, 69-77.

Setiawan, D., & Mufarrihah, I. (2024). Implementasi Metode Kriptografi Advanced Encryption Standard 128 Bit (Aes 128 Bit) Pada Keamanan File Dokumen. Inovate : Jurnal Ilmiah Inovasi Teknologi Informasi, 8(2), 74–81.

Shita, R. T. & Hin, L. L., 2021. Implementasi Algoritma Kriptografi AES 128 Bit dan Elgamal Untuk Pengamanan E-mail Pada Bandara Internasional Sultan Mahmud Bahruddin II Palembang. Volume 1, pp. 1-11.

Simamarta, J., S. & Rahim, R., 2019. *Kriptografi Teknik Kea444manan Data Dan Informasi*. 1 ed. Yogyakarta: Andi.