3rd Seminar Nasional Mahasiswa Fakultas Teknologi Informasi (SENAFTI)
30 Agustus 2023 – Jakarta, Indonesia
Volume 2, Nomor 2, September 2023 - ISSN 2962-8628 (*online*)

IMPLEMENTASI ALGORITME AES 128 UNTUK KEAMANAN FILE BERBASIS WEB

Arif Yaomulfurqqan[1*], Wahyu Pramusinto[2]

[1*,2]Teknik Informatika, Fakultas Teknologi Informasi, Universitas Budi Luhur, Jakarta Selatan, Indonesia

Email: [1*]arifyaumul3@gmail.com, [2]wahyu.pramusinto@budiluhur.ac.id
(* : corresponding author)

Abstrak-Data sensitif seperti data project merupakan informasi yang penting dan harus dilindungi dari akses oleh pihak yang tidak berwenang. PT Enam Lima Ihsan perlu memiliki sistem keamanan yang handal untuk melindungi data sensitif tersebut. Pertanyaannya adalah, bagaimana cara melindungi data tersebut agar tidak dicuri? Dan bagaimana cara mengembalikan data yang telah dienkripsi menjadi data asli tanpa mengubah isinya? Salah satu solusi untuk melindungi data sensitif adalah dengan menggunakan algoritma kriptografi Advanced Encryption Standard (AES) 128. Algoritma ini dapat digunakan untuk mendekripsi data yang telah dienkripsi sebelumnya, sehingga mencegah pencurian atau kebocoran data. AES 128 adalah pilihan yang tepat karena mampu melindungi data dengan baik dan memenuhi standar keamanan yang tinggi. Dalam implementasi ini, dokumen yang dapat digunakan adalah dokumen dengan format docx, xlsx, pptx, dan pdf. Sistem yang dikembangkan memastikan bahwa data dalam dokumen tersebut tidak dapat dibaca atau dimodifikasi oleh pihak yang tidak berwenang. Metodologi penelitian yang digunakan melibatkan pengembangan sistem, analisis keamanan sistem, dan pengujian untuk memvalidasi hasil implementasi. Hasil penelitian ini menunjukan AES 128 pada PT Enam Lima Ihsan dapat melindungi data project dan data sensitive lainnya dengan baik sehingga keamanan dapat bertambah. Ukuran text hasil enkripsi yang diperoleh sama dengan ukuran text asli. Rata-rata waktu proses enkripsi yaitu 28,61 s sedangkan rata-rata proses dekripsi 27,88 s. Proses enkripsi pada algoritma AES 128 lebih membutuhkan waktu lama dibandingkan proses dekripsinya. Implementasi ini merupakan solusi yang efektif untuk menjaga keamanan data sensitif dalam PT Enam Lima Ihsan

Kata Kunci: Data project, *Advanced Encryption Standard*, Sistem keamanan, Enkripsi dan Dekripsi, File

IMPLEMENTATION OF AES 128 ALGORITHM FOR WEB-BASED FILE SECURITY

Abstract-*Sensitive data such as project data is important information and must be protected from access by unauthorized parties. PT Enam Lima Ihsan needs to have a reliable security system to protect this sensitive data. The question is, how to protect the data from being stolen? And how do you restore encrypted data to original data without changing its contents? One solution to protect sensitive data is to use the Advanced Encryption Standard (AES) 128 cryptographic algorithm. This algorithm can be used to decrypt data that has been previously encrypted, thereby preventing data theft or leakage. AES 128 is the right choice because it is able to protect data properly and meets high security standards. In this implementation, documents that can be used are documents in docx, xlsx, pptx, and pdf formats. The developed system ensures that the data in the document cannot be read or modified by unauthorized parties. The research methodology used involves system development, system security analysis, and testing to validate implementation results. The results of this research demonstrate that AES 128 at PT Enam Lima Ihsan is capable of effectively safeguarding project data and other sensitive information, thereby enhancing security. The size of the encrypted text obtained is the same as the original text size. The average encryption processing time is 28.61 seconds, while the average decryption processing time is 27.88 seconds. The encryption process in the AES 128 algorithm requires more time compared to the decryption process. This implementation is an effective solution for maintaining the security of sensitive data within PT Enam Lima Ihsan.*

Keywords*: Data project, Advanced Encryption Standard, Security system, Encryption and Decryption, File*

1. PENDAHULUAN

Pada perkembangan teknologi saat ini banyak kita temukan pencurian data-data pribadi maupun perusahaan yang digunakan untuk kepentingan lain. Dimana data merupakan komponen penting dalam sebuah perusahaan. Kerahasiaan dari sebuah data merupakan hal mutlak yang dibuat untuk menjaga agar informasi yang tersimpan tidak dapat dibaca atau dibuka oleh pihak yang tidak berhak.[1]

PT Enam Lima Ihsan adalah perusahaan yang bergerak dalam bidang umum dan jasa dengan menitik beratkan pada solusi Teknologi Informasi. Perusahaan ini juga didukung dengan personil berpengalaman, bekerja

dengan basis proyek dan dapat menyediakan tenaga ahli professional yang memiliki keterampilan Teknis dan juga Bisnis.

Kriptografi adalah ilmu dan seni untuk menjaga kerahasiaan pesan dengan cara menyandikannya kedalam bentuk yang tidak dapat dimengerti lagi maknanya. Kriptografi adalah sebuah bidang ilmu yang memfokuskan pada teknik-teknik matematika yang terkait dengan keamanan data dan informasi, termasuk aspek-aspek seperti keabsahan data, integritas data, dan autentikasi data[2].

Dalam ilmu kriptografi, terdapat dua buah proses yaitu melakukan enkripsi dan dekripsi.[3] Enkripsi merujuk pada proses mengubah data menjadi bentuk yang sulit untuk dipahami atau dibaca, yang disebut sebagai teks terenkripsi atau *Chipertext* Sedangkan dekripsi merupakan proses sebaliknya, yaitu mengembalikan data yang telah dienkripsi menjadi bentuk aslinya atau teks awal, yang disebut sebagai teksasli atau *Plaintext*.[4]

Kriptografi tidak hanya berperan dalam menjaga keamanan pesan yang dikirimkan, tetapi juga memiliki beberapa tujuan yang penting dalam keamanan. Tujuan-tujuan tersebut adalah memastikan kerahasiaan pesan selama proses pengiriman, menjamin integritas data dengan mencegah modifikasi saat pengiriman, melakukan identifikasi yang jelas antara pengirim dan penerima pesan untuk autentikasi, serta mencegah pihak yang terlibat untuk menyangkal pengiriman atau penerimaan pesan[5]

Dalam penelitian ini, algoritma AES dipilih karena hasil penelitian sebelumnya menunjukkan bahwa kecepatan enkripsi dan dekripsi AES masih lebih unggul daripada beberapa algoritma lain yang telah diuji[6]. Pada penelitian sebelumnya yang dilakukan oleh Anggraeni dkk, 2020 dengan judul *Implementasi Kriptografi Dengan Algoritma Advanced Encryption Standard (AES) 128 Bit dan Steganografi menggunakan Metode End of File (EOF) berbasis Java Pada Desktop Pada Diinas Pendidikan Kabupaten Tangerang* bahwa algoritma ini mampu menjaga keamanan dan kerahasian data, sehingga pada penelitian menggunakanalgoritma AES namun dengan berbasis PHP WEB dikarenakan lebih fleksibel dalam pengaksesan dan penggunaannya.[7]

Advanced Encryption Standard (AES) adalah sebuah algoritme kriptografi simetris yang digunakan untuk melindungi data informasi. Algoritme ini merupakan standar enkripsi yang menggunakan kunci simetris. Beberapa mode operasi yang dapat diterapkan pada algoritme penyandi blok AES antara lain adalah *Electronic Code Book* (ECB), *Cipher Block Chaining* (CBC), *Cipher Feedback* (CFB), dan *Output Feedback* (OFB)[8], Algoritma AES (*Advanced Encryption Standard)* ditemukan oleh Vincent Rijnmen dan Joan Daeman dari Belgia. Evaluasi terhadap Rijndael, yang merupakan bagian dari AES, mencakup beberapa poinpenting. Pertama, belum ada jenis serangan yang diketahui yang mampu memecahkan algoritma Rijndael. Kedua, algoritma ini menggunakan S-Box nonlinier, yang meningkatkan tingkat keamanannya. Dan yang ketiga, Rijndael terkenal karena efisiensinya yang tidak memakan banyak sumber daya komputasi[9].

2. METODE PENELITIAN

2.1 Kriptografi

Kriptografi berasal dari bahasa Yunani, Crypto berarti rahasia (secret) dan Graphia berarti tulisan (writing). Adapun pengertian kriptografi adalah ilmu yang mempelajari teknik-teknik matematika yang saling berkaitan dengan aspek keamanan data dan informasi seperti autentifikasi data, keabsahan data, serta integritas data[10]. Proses enkripsi melibatkan transformasi pesan asli yang akan dikirim menjadi informasiacak, menggunakan kunci yang hanya diketahui oleh pengirim dan penerima. Kunci ini memiliki peran penting karena memungkinkan penerima untuk mengubah kembali teks terenkripsi (*ciphertext*) menjadi teks asli (*plaintext*). Metode yang digunakan pada pengimplementasian algoritma AES yaitu dengan menggunakan kunci yang sama pada proses enkripsi dan dekripsinya sehingga kunci itu harus bersifat privatedimana hanya pengirim dan Penerima yang mengetahui kunci tersebut sehingga dibutuhkan transmisi pengiriman kunci yang aman.

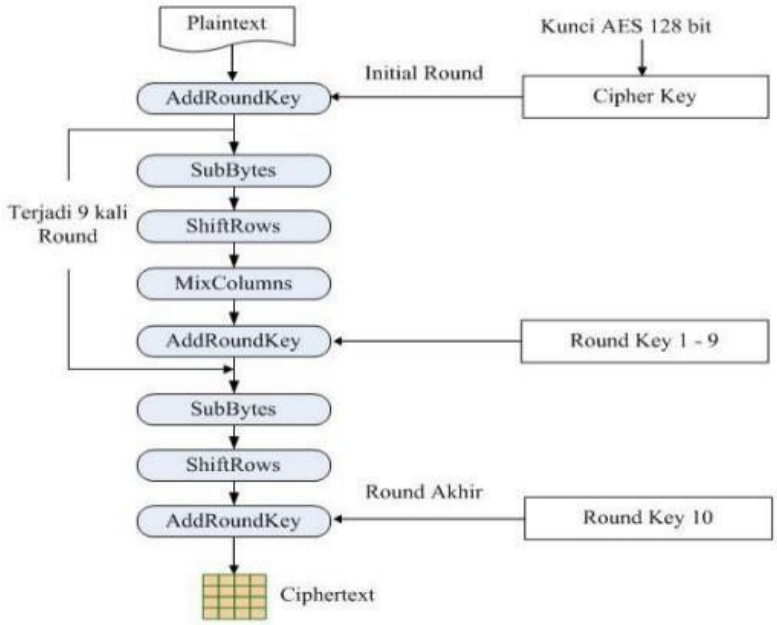
Proses enkripsi AES adalah transformasi terhadap state secara berulang dalan beberapa ronde. State yang menjadi keluaran ronde k menjadi masukan untuk ronde ke k+1. Secara ringkas algoritma deskripsi AES merupakan kebalikan algoritma enkripsi AES. Algoritma deskripsi AES menggunakan transformasi invers semua transformasi dasar yang digunakan pada algooritma enkripsi AES [11]

2.2 Proses Enkripsi *Advanced Encryption Standard* (AES) 128 Bit

Secara umum, proses enkripsi AES-128 dengan kunci 128 bit dapat dijelaskan sebagai berikut:

a. *AddRoundKey*: melakukan XOR antara state awal (*plainteks*) dengan *cipherkey*. Pada Tahap ini disebut juga initial *round.*
b. *Round*: memiliki Putaran sebanyak Nr – 1 kali. Proses yang dilakukan pada setiap putaran adalah:
   1) *SubBytes*: substitusi *byte* dengan menggunakan tabel substitusi (S-box).
   2) *ShiftRows*: pergeseran baris-baris array state secara wrapping.
c. MixColumns berfungsi untuk mengacak data pada masing-masing kolom array state dengan persamaan sebagai berikut: A(x) = {03}x2 + {01}x2 + {01}x2 + {02} (1).
d. AddRoundKey digunakan untuk melakukan XOR antara state sekarang round key.
e. AddRoundKey digunakan untuk melakukan XOR antara state sekarang round key.
   1) *SubBytes*
   2) *Shiftrows*
   3) *AddRoundKey*
f. Pada proses terakhir akan menghasilkan karakter atau teks yang berbentuk chipertext.

Dibawah ini berikut Gambar 1 Proses Enkripsi AES-128 bit



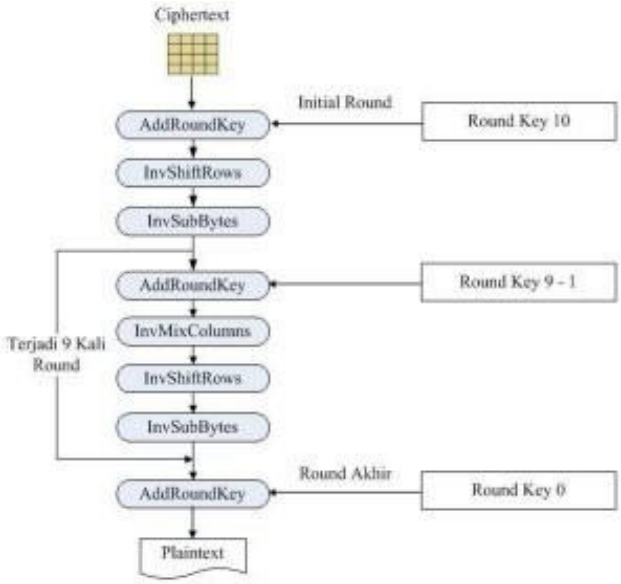
Gambar 1. Proses Enkripsi AES-128 bit

2.3 Proses Dekripsi *Advanced Encryption Standard* (AES) 128 Bit

Proses dekripsi AES-128 dengan kunci AES-128 bit dijelaskan sebagai berikut:

a. *InvShiftRows*: melakukan pergeseran bit ke kanan pada setiap blok baris.
b. *InSubBytes*: Setiap elemen pada state dipetakan dengan tabel Inverse S-Box.
c. *InvMixColumns*: Setiap kolom dalam state dikalikan dengan matriks AES.
d. *AddRoundKey*: Mengombinasikan state array dan round key dengan hubungan XOR
e. Pada proses terakhir akan menghasilkan karakter atau teks asli (*plaintext*).

Dibawah ini berikut Gambar 2 Proses Dekripsi AES-128 bit



Gambar 2. Proses Dekripsi AES-128 bit

2.4 Pengujian Sistem

Pengujian ada beberapa tahapan untuk menentukan apakah setiap fitur dari elemen yang disertakan dalam aplikasi dapat bekerja dengan baik. Berikut adalah rancangan pengujian pada tebel 1 dibawah ini

Tabel 1. Rancangan Pengujian

No	Pengujian	Hasil yang diharapkan
1	Tombol Login	Mengakses ke menu utama
2	Tombol Dashboard	Menampilkan halaman Dashboard
3	Tombol Enkripsi	Menampilkan halaman Enkripsi dan bisa menenkripsi file
4	Tombol Reset	Untuk Menghapus semua isi di Textbox
5	Tombol Dekripsi	Menampilkan halaman Dekripsi dan bisa Dekripsi file yang telah di Enkripsi
6	File	Menampilkan file yang telah di Enkripsi
7	Tentang Aplikasi	Menampilkan Penjelasan tentang Aplikasi

2.5 Spesifikasi *Database*

Dibawah ini terdapat struktur-struktur dari spesifikasi database yang diterapkan untuk mengembangkan aplikasi ini. Tabel 1 merangkum spesifikasi database file, sementara Tabel 2 memuat spesifikasi database pengguna (users). Berikut Spesifikasi *Database* pada tabel 2 dan 3 dibawah ini

a. Tabel *User*

Nama Database : Kriptografi
Nama Tabel : User
Media : Hardisk
Primary Key : Username

Tabel 2. Data User

NO	Nama *Field*	*Type*	*Length*	*Keterangan*
1	Username	Varchar	15	Email Pengguna
2	Password	Varchar	100	*Password*
3	Fullname	Varchar	50	Nama Pengguna
4	Job_title	Varchar	50	Keterangan jabatan *user*
5	Join_date	Timestamp	-	Keterangan kapan *user* terdaftar di aplikasi
6	Last_activity	Timestamp	-	Keterangan kapan *user* terakhir kali aktif di aplikasi
7	Status	Enum	-	Keterangan statur *user*

b. Tabel *File*

Nama *Database* : Kriptografi
Nama Tabel : File
Media : Hardisk
Primary key : File

Tabel 3. Data File

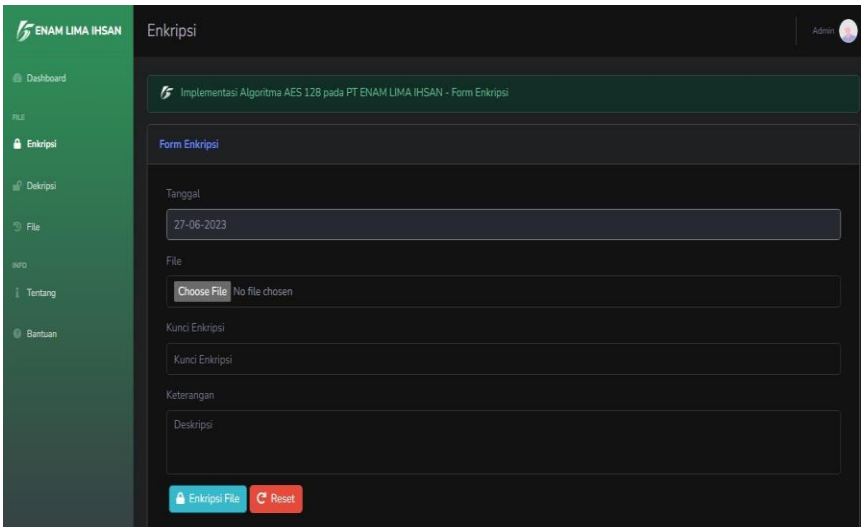
No	Nama *Field*	*Type*	*Length*	Keterangan
1	Id_file	Int	11	Berisi id *file*
2	Username	Varchar	15	Berisi *Username* untuk *user*
3	File_name_source	Varchar	255	Berisi keterangan nama *file* sebelum dienkripsi
4	File_name_finish	Varchar	255	Berisi keterangan nama *file* sesudah dienkripsi
5	File_url	Varchar	255	Berisi keterangan lokasi penyimpanan *file*
6	File_size	Float	-	Berisi keterangan ukuran file
7	Password	Varchar	16	Berisi *Password file*
8	Tgl_upload	Timestamp	-	Berisi keterangan upload *file*
9	Status	Enum	-	Berisi keterangan status *user*
10	Keterangan	varchar	255	Berisi keterangan *file*

3. HASIL DAN PEMBAHASAN

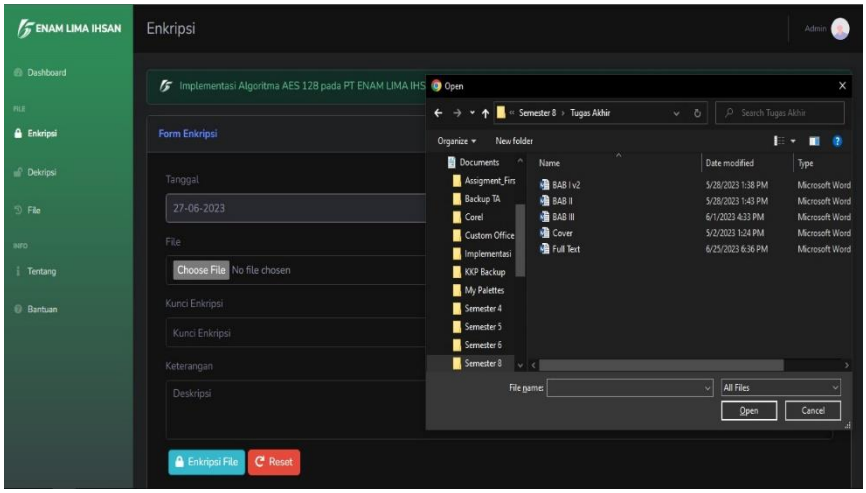
3.1 Implementasi Metode

a. Proses Enkripsi

Proses Enkripsi Untuk memulai enkripsi, pengguna harus masuk ke menu "Form Enkripsi", lalu pilih *file* yang akan dienkripsi setelah memilih file pengguna harus memasukan kunci enkripsi dan keteranganlalu mengklik *button* Enkripsi File. Berikut adalah tampilan proses enkripsi pada gambar 3 dan 4.



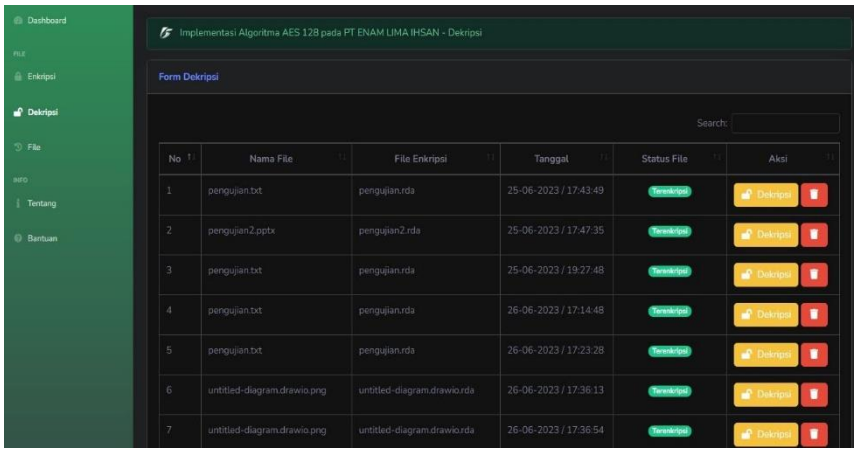
Gambar 3. Form Enkripsi



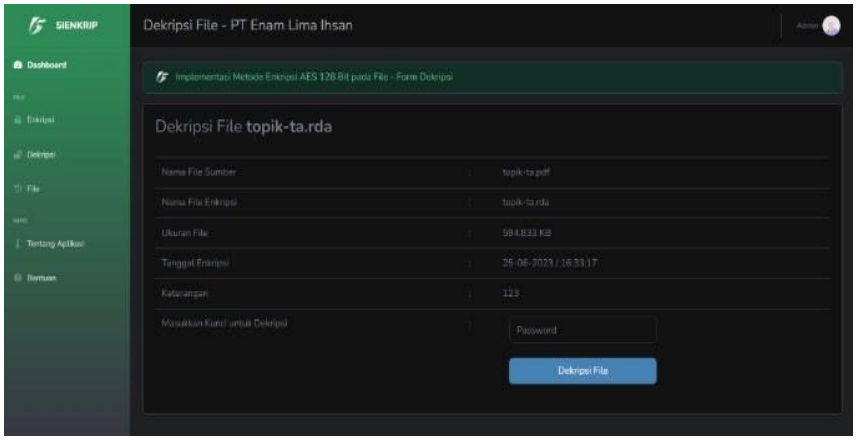
Gambar 4. Proses Enkripsi

b. Proses Dekripsi

Proses Dekripsi Untuk memulai proses dekripsi, pengguna tinggal memilih file, Kemudian pengguna dapat memilih file yang ingin didekripsi dengan mengklik tombol dekripsi. Berikut adalah tampilan proses dekripsi pada gambar 5 dan 6.



Gambar 5. Form Dekripsi



Gambar 6. Proses Dekripsi

c. Proses Dekripsi

Setelah proses enkripsi selesai, kita mencoba membuka file yang telah dienkripsi. Berikut adalah hasilnya pada gambar 7 dibawah ini

Gambar 7. Tampilan hasil enkripsi

3.2 Hasil Pengujian

Pada tahap ini, dilakukan pengujian pada aplikasi yang telah dibuat untuk membandingkan ukuran file hasil proses enkripsi dan dekripsi dari metode *Advanced Encryption Standard* (AES 128). Tujuan dari pengujian ini adalah untuk mengetahui apakah ukuran file hasil enkripsi dan dekripsi sama atau berbeda.

Proses keamanan AES 128 dengan ekspansi Kunci, pertama mengurutkan kunci ke dalam blokberukuran 128bit (16 kode ASCII). Lalu ubah kunci kedalam bentuk heksadesimal

a	r	i	f	a	r	i	f	a	r	i	f	a	r	i	f
61	72	69	66	61	72	69	66	61	72	69	66	61	72	69	66

Gambar 8. Urut Kunci Ke ASCII

Lalu susun kunci yang diubah kedalam bentuk heksadesimal kedalam state berukuran 4 x 4

61	61	61	61
72	72	72	72
69	69	69	69
66	66	66	66

Gambar 9. State Kunci

Proses mendapatkan kolom pertama hingga ke sepuluh dengan menggunakan serangkaian operasi dengan melibatkan fungsi RotWord, SubByte, dan XOR antara kolom pertama dari kunci ronde ke-0 dengan hasil dari SubBytes, kemudian hasilnya di-XOR-kan dengan RCon. Langkah ini menghasilkan hasil dari ronde ke-10.

0A	1A	00	0C
00	0B	14	00
00	08	0C	04
11	1A	05	1B

Gambar 10. Hasil Ronde 10

Proses Enkripsi text “pt enamlimaihsan” dengan kunci yang telah dibangkitkan pada proses sebelumnya. Lakukan penubahan text ke dalam ASCII sebagai berikut.

p	t	sp	e	n	a	m	l	i	m	a	i	h	s	a	n
70	74	20	65	6E	61	6D	6C	69	6D	61	69	68	73	61	6E

Gambar 11. Convert ke ASCII

Kemudian lakukan sususan 16 byte pertama dari plaintext lalu lakukan XOR antara plaintext dengan Roundkey 0. Proses ini dinamakan ADDroundkey.

70	6E	69	68
74	61	6D	73
20	6D	61	61
65	6C	69	6E

Gambar 12. Hasil Pra-ronde ADDroundkey

Kemudian lakukan transformasi, yaitu SubBytes, ShiftRows, MixColumns, dan AddRoundKey.

70	6E	69	68	XOR	61	61	61	61	=	11	0F	8	9
74	61	6D	73		72	72	72	72		6	13	1F	11
20	6D	61	61		69	69	69	69		49	4	8	18
65	6C	69	6E		66	66	66	66		3	0A	0F	8

Gambar 12. Hasil Pra-ronde ADDroundkey

Kemudian lakukan transformasi, yaitu SubBytes, ShiftRows, MixColumns, dan AddRoundKey.

22	3B	38	54	→	82	76	30	01
24	28	31	3C	→	6F	7D	C0	82
3D	48	3D	20	→	3B	F2	30	AD
30	2C	20	32	→	7B	67	76	30

Gambar 13. Hasil pra-round disubtitusikan dengan nilai pada tabel S-Box

82	76	30	01		82	76	30	01
6F	7D	C0	82		7D	C0	82	6F
3B	F2	30	AD		3B	AD	30	F2
7B	67	76	30		30	7B	67	76

Gambar 13. Hasil ShiftRows pada hasil dari subtitusi SubBytes

82	76	30	01	X	2	3	1	1	=	E2	3A	A2	19
7D	C0	82	EB		1	2	3	1		87	C2	A2	03
3B	AD	30	F2		1	1	2	3		41	3A	3B	40
30	7B	67	76		3	1	1	2		39	EA	FA	9C

Gambar 14. Transformasi MixColumns

MixColumns					RoundKey Ke-					AddRoundKey			
E2	3A	A2	19	XOR	20	41	20	41	=	C2	7B	82	58
87	C2	A2	03		8B	F9	8B	F9		C	3B	29	FA
41	3A	3B	40		5A	33	5A	33		1B	9	61	73
39	EA	FA	9C		89	EF	89	EF		B0	5	73	73

Gambar 15. XOR antara hasil MixColumns

35	FC	18	4E
C1	F4	79	B1
03	5A	CD	6D
C3	04	E4	5C

Gambar 15. Hasil Enkripsi

Dari proses enkripsi tersebut *ciphertext* yang dihasilkan adalah Dan hasil dari enkripsi dengan algoritma AES-128 menghasilkan chipertext sebagai berikut 35 C1 03 C3 FC F4 5A 04 18 79 CD E4 4E B1 6D 5C

Ciphertext yang dihasilkan tidak dapat dimengerti dan dipahami dikarenakan text asli sudah dilakukanmetode enkripsi sehingga pesan terjaga kerahasiannya.

Selain itu juga melakukan pengukuran waktu yang dibutuhkan untuk proses enkripsi dan dekripsi file. Berikut adalah hasil dari proses enkripsi dan dekripsi pada tabel 4 dan 5

Tabel 4. Hasil pengujian Enkripsi

No	Dokumen	Ukuran asli dokumen	Ukuran dokumen hasil Enkripsi	Status	
				Enkripsi	Waktu
1	Nama Karyawan.xlsx	9kb	9kb	Berhasil	0.21 detik
2	Topik TA.pdf	595kb	595kb	Berhasil	14.94 detik
3	Final.docx	4,847kb	4,847kb	Berhasil	126.63 detik
4	Pengujian.txt	4kb	4kb	Berhasil	0.12 detik
5	Pengujian.pptx	43kb	43kb	Berhasil	1.15 detik

Tabel 5. Hasil pengujian Dekripsi

No	Dokumen	Ukuran asli dokumen	Ukuran dokumen hasil Dekripsi	Status	
				Dekripsi	Waktu
1	Nama Karyawan.xlsx	9kb	9kb	Berhasil	0.21 detik
2	Topik TA.pdf	595kb	595kb	Berhasil	13.84 detik
3	Final.docx	4,847kb	4,847kb	Berhasil	124.06 detik
4	Pengujian.txt	4kb	4kb	Berhasil	0.11 detik
5	Pengujian2.pptx	43kb	43kb	Berhasil	1.21 detik

4. KESIMPULAN

Penelitian ini menunjukan AES 128 pada PT Enam Lima Ihsan dapat melindungi data project dan data sensitive lainnya dengan baik sehingga keamanan dapat bertambah. Ukuran text hasil enkripsi yang diperolehsama dengan ukuran text asli. Rata-rata waktu proses enkripsi yaitu 28,61 s sedangkan rata-rata proses dekripsi 27,88 s. Proses enkripsi pada algoritma AES 128 lebih membutuhkan waktu lama dibandingkan proses dekripsinya.

Melalui sejumlah kesimpulan ini, dapat disimpulkan bahwa pengembangan program aplikasi keamanan file berbasis web dengan menggunakan metode *Advanced Encryption Standard* (AES-128) untuk melindungi file di PT Enam Lima Ihsan telah berhasil menghasilkan suatu solusi yang dapat menjaga keutuhan ukuran dokumen asli, memiliki keterbatasan dalam format dokumen yang dapat dienkripsi, dan menjaga ukuran file asli yang telah melalui proses enkripsi tanpa mengalami perubahan yang berarti.

DAFTAR PUSTAKA

[1] A. Prameshwari dan N. P. Sastra, "Implementasi Algoritma Advanced Encryption Standard (AES) 128 Untuk Enkripsi dan Dekripsi File Dokumen," *Eksplora Inform.*, vol. 8, no. 1, hal. 52, 2018, doi:10.30864/eksplora.v8i1.139.

[2] H. Wijaya, "Implementasi Kriptografi AES-128 Untuk Mengamankan URL (Uniform Resource Locator) dari SQL Injection," *Akad. J.*, vol. 17, no. 1, hal. 8–13, 2020.

[3] A. Eka Putri, A. Kartikadewi, dan L. A. Abdul Rosyid, "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," *Appl. Inf. Syst. Manag.*, vol. 3, no.2, hal. 69–78, 2021, doi: 10.15408/aism.v3i2.14722.

[4] M. A. Sutejo dan M. Hardjianto, "Pengamanan File Pendaftaran Siswa Baru Menggunakan Metode Algoritme Rc4 Di Tk Nurul Irfan Security of New Student Registration Files Using the Rc4 Algorithm Method in Tk Nurul Irfan," *Semin. Nas. Mhs. Fak. Teknol. Inf. Jakarta-Indonesia*, vol. 4, no. September,hal. 394–401, 2022.

[5] N. W. Hidayatulloh, M. Tahir, H. Amalia, N. A. Basyar, A. F. Prianggara, dan M. Yasin, "Mengenal Advance Encrytion Standard (AES) Sebagai Algoritma Kriptografi Dalam Mengamankan Data," *Digit. Transform. Technol.*, vol. 3, no. 1, hal. 1–10, 2023.

[6] A. Ignasius dan D. V. Shaka Yudha Sakti, "Penerapan Algoritma Aes (Advance Encryption Standart) 128Untuk Enkripsi Dokumen Di Pt. Gunung Geulis Elok Abadi," *Skanika*, vol. 5, no. 1, hal. 1–10, 2022, doi:10.36080/skanika.v5i1.2118.

[7] Eka Putri, A., Kartikadewi, A., & Abdul Rosyid, L. A. (2021). ImplementasiKriptografi 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 System and Management (AISM), 3(2), 69–78. https://doi.org/10.15408/aism.v3i2.14722

[8] F. A. Sitorus, N. B. Nugroho, dan U. F. S. S. Pane, "Implementasi Algoritma Advanced Encryption Standard (AES) 128 Bit untuk Keamanan Data Transaksi Penjualan Pada PT. Mitsubishi Electric Indonesia," *J. CyberTech*, no. x, hal. 1–15, 2020, [Daring]. Tersedia pada: https://ojs.trigunadharma.ac.id/

[9] I. A. R. Simbolon, I. Gunawan, I. O. Kirana, R. Dewi, dan S. Solikhun, "Penerapan Algoritma AES 128- Bit dalam Pengamanan Data Kependudukan pada Dinas Dukcapil Kota Pematangsiantar," *J. Comput. Syst.Informatics*, vol. 1, no. 2, hal. 54–60, 2020.

[10] R. Andriyanto, K. Khairijal, dan D. Satria, "Penerapan Kriptografi AES Class Untuk Pengamanan URL WEBSITE Dari Serangan SQL INJECTION," *J. Unitek*, vol. 13, no. 1, hal. 34–48, 2020, doi: 10.52072/unitek.v13i1.153.

[11] L. Mustika, "Implementasi Algoritma AES Untuk Pengamanan Login Dan Data Customer Pada E- Commerce Berbasis Web," *JURIKOM (Jurnal Ris. Komputer)*, vol. 7, no. 1, hal. 148, 2020, doi:10.30865/jurikom.v7i1.1943.