JURNAL SISTEM INFORMASI TGD
Volume 5, Nomor 1, Januari 2026, Hal 428-437
P-ISSN : 2828-1004 ; E-ISSN : 2828-2566
https://ojs.trigunadharma.ac.id/index.php/jsi

Analisis dan Implementasi Algoritma AES untuk Pengamanan Dokumen Pemerintahan Berbasis Website.

Zaimah Panjaitan[1], Muhammad Zaki Nasri Nasution[2], Deski Helsa Pane[3], Khairi Ibnutama[4]
[1,2,3] Sistem Informasi, STMIK Triguna Dharma
Email: [1]zaimahp09@gmail.com, [2]muhammadzakinasrinst@gmail.com, [3]deskihelsa@gmail.com, [4]mr.ibnutama@gmail.com
Email Penulis Korespondensi: zaimahp09@gmail.com

Abstrak
Keamanan dokumen pemerintahan merupakan aspek penting dalam mendukung tata kelola pemerintahan yang transparan dan terpercaya, khususnya pada sistem pengelolaan dokumen berbasis website. Dokumen perencanaan pembangunan, seperti hasil kesepakatan Musyawarah Perencanaan Pembangunan (MUSRENBANG), memiliki tingkat kerahasiaan tinggi sehingga memerlukan mekanisme pengamanan yang andal. Penelitian ini bertujuan untuk menganalisis dan mengimplementasikan algoritma Advanced Encryption Standard (AES) dalam pengamanan dokumen pemerintahan berbasis website. Metode penelitian yang digunakan meliputi analisis kebutuhan sistem, perancangan arsitektur aplikasi, serta implementasi algoritma AES pada proses enkripsi dan dekripsi dokumen. Pengujian sistem dilakukan dengan mengukur waktu proses enkripsi dan dekripsi pada berbagai ukuran file dokumen untuk mengevaluasi kinerja algoritma yang diterapkan. Hasil penelitian menunjukkan bahwa algoritma AES mampu memberikan tingkat keamanan yang baik terhadap dokumen pemerintahan tanpa memberikan dampak signifikan terhadap kinerja sistem berbasis website. Selain itu, sistem yang dikembangkan mampu menjaga kerahasiaan data dokumen dari akses tidak sah. Kesimpulan dari penelitian ini adalah bahwa penerapan algoritma AES efektif digunakan sebagai solusi pengamanan dokumen pemerintahan berbasis website dan dapat diimplementasikan sebagai model pengamanan data pada sistem e-government tingkat lokal..
Kata Kunci: Algoritma AES, Keamanan Data, Dokumen Pemerintahan, Enkripsi, Aplikasi Berbasis Website.

Abstract
The security of government documents is a critical aspect in supporting transparent and trustworthy governance, particularly in web-based document management systems. Development planning documents, such as the results of the Development Planning Deliberation (MUSRENBANG), contain highly confidential information and therefore require reliable security mechanisms. This study aims to analyze and implement the Advanced Encryption Standard (AES) algorithm for securing government documents in a web-based environment. The research methodology includes system requirement analysis, application architecture design, and the implementation of the AES algorithm in the document encryption and decryption processes. System testing was conducted by measuring encryption and decryption processing time across various document file sizes to evaluate the performance of the implemented algorithm. The results indicate that the AES algorithm provides a strong level of security for government documents without causing significant performance degradation in web-based systems. Furthermore, the developed system is capable of protecting document confidentiality from unauthorized access. This study concludes that the implementation of the AES algorithm is effective as a solution for securing government documents in web-based applications and can be adopted as a data security model for local e-government systems.
Keywords*: AES Algorithm, Data Security, Government Documents, Encryption, Web-Based Application.*

1. PENDAHULUAN

Perkembangan teknologi informasi telah mendorong instansi pemerintahan untuk mengadopsi sistem informasi berbasis website dalam pengelolaan dan penyimpanan dokumen. Digitalisasi dokumen memberikan kemudahan dalam proses pengarsipan, distribusi, dan akses data secara efisien, namun di sisi lain juga meningkatkan risiko ancaman keamanan informasi seperti pencurian data, akses tidak sah, dan manipulasi dokumen digital[1][2]. Dokumen pemerintahan yang bersifat strategis memerlukan mekanisme pengamanan yang mampu menjamin kerahasiaan dan integritas data agar tidak disalahgunakan oleh pihak yang tidak berwenang[3].Salah satu dokumen penting dalam sistem pemerintahan adalah dokumen perencanaan pembangunan, seperti hasil kesepakatan Musyawarah Perencanaan Pembangunan (MUSRENBANG). Dokumen ini memuat informasi strategis terkait prioritas program dan kebijakan pembangunan yang menjadi dasar pengambilan keputusan pemerintah. Apabila dokumen tersebut tidak dilindungi dengan baik dalam sistem berbasis website, maka risiko kebocoran informasi dapat berdampak pada terganggunya proses perencanaan dan menurunnya kepercayaan publik terhadap tata kelola pemerintahan [4][5].

Kriptografi merupakan solusi yang umum digunakan untuk mengamankan data digital. Algoritma Advanced Encryption Standard (AES) adalah algoritma kriptografi simetris yang telah diakui secara luas karena tingkat keamanannya yang tinggi dan efisiensinya dalam proses enkripsi dan dekripsi data [6][7]. AES banyak diterapkan dalam pengamanan data dan dokumen berbasis web, termasuk pengamanan file digital, sistem transaksi, dan sistem informasi pemerintahan [8][9]. Beberapa penelitian menunjukkan bahwa algoritma AES dengan variasi panjang kunci seperti AES-128 dan AES-256 mampu memberikan perlindungan yang kuat terhadap data sensitif tanpa memberikan beban komputasi yang signifikan pada sistem [10]. Penelitian terdahulu telah membahas implementasi algoritma AES dalam pengamanan dokumen berbasis web pada berbagai bidang, seperti sistem pendidikan, transaksi digital, serta pengelolaan dokumen

JURNAL SISTEM INFORMASI TGD
Volume 5, Nomor 1, Januari 2026, Hal 428-437
P-ISSN : 2828-1004 ; E-ISSN : 2828-2566
https://ojs.trigunadharma.ac.id/index.php/jsi

umum. Beberapa studi juga mengombinasikan AES dengan metode keamanan lain atau menganalisis kinerja algoritma berdasarkan waktu proses enkripsi dan dekripsi terhadap ukuran file tertentu [11][12][13]. Meskipun demikian, kajian yang secara khusus membahas analisis dan implementasi algoritma AES untuk pengamanan dokumen pemerintahan berbasis website, terutama pada dokumen perencanaan pembangunan, masih terbatas dan belum banyak dieksplorasi secara mendalam [14].

Berdasarkan permasalahan tersebut, penelitian ini bertujuan untuk melakukan analisis dan implementasi algoritma AES dalam pengamanan dokumen pemerintahan berbasis website. Penelitian ini diharapkan dapat menghasilkan sistem pengamanan dokumen yang efektif dan efisien serta dapat dijadikan sebagai model pengamanan data pada pengembangan sistem e-government di tingkat lokal maupun instansi pemerintahan lainnya.

2. METODOLOGI PENELITIAN

2.1 Tahapan Penelitian

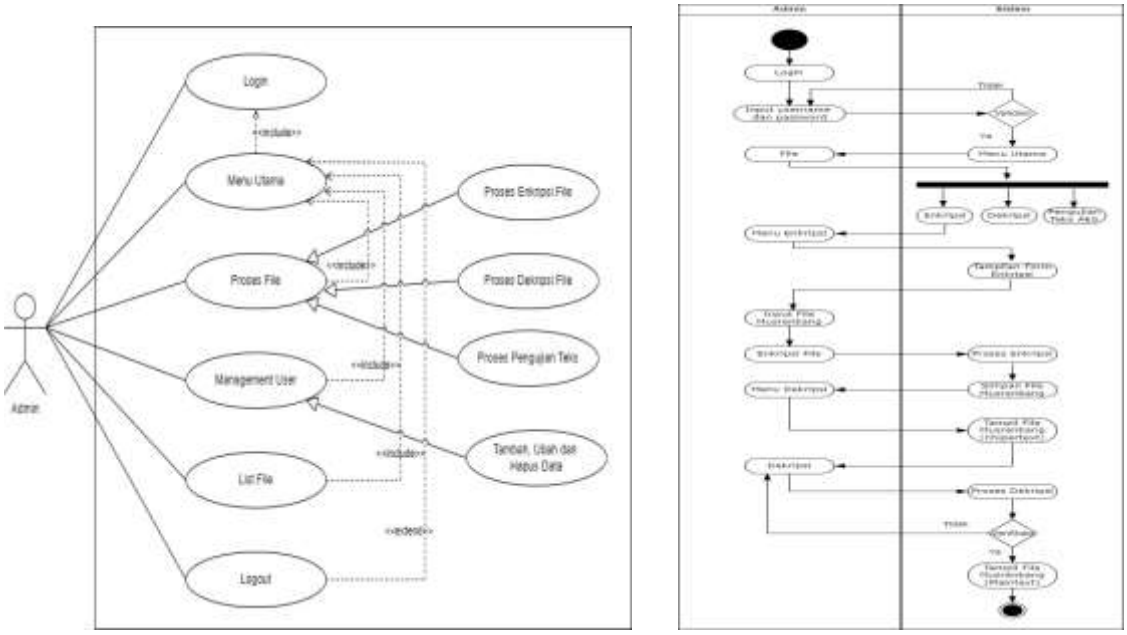
Penelitian ini menggunakan metode research and development (R&D) dengan pendekatan eksperimental, yang bertujuan untuk menganalisis dan mengimplementasikan algoritma Advanced Encryption Standard (AES) dalam pengamanan dokumen pemerintahan berbasis website. Metode ini dipilih karena penelitian berfokus pada pengembangan sistem aplikasi serta pengujian kinerja algoritma kriptografi yang diterapkan. Adapun tahapan dari penelitian ini adalah sebagai berikut :

1. Analisis Kebutuhan Sistem

Pada tahap ini dilakukan analisis terhadap kebutuhan sistem pengamanan dokumen pemerintahan berbasis website. Analisis meliputi jenis dokumen yang diamankan, alur pengelolaan dokumen, serta potensi ancaman keamanan yang dapat terjadi pada sistem web. Selain itu, ditentukan kebutuhan fungsional sistem, seperti proses unggah dokumen, enkripsi, dekripsi, dan manajemen hak akses pengguna.

2. Perancangan Sistem

Tahap perancangan sistem mencakup desain arsitektur aplikasi berbasis website serta perancangan alur proses enkripsi dan dekripsi dokumen. Algoritma AES dirancang untuk bekerja pada proses pengamanan file dokumen sebelum disimpan ke dalam sistem. Perancangan juga meliputi desain antarmuka pengguna (user interface) serta pemodelan alur sistem untuk menggambarkan proses kerja sistem secara keseluruhan. Berikut gambaran sistem pada Usecase Diagram :



Gambar 1. Perancangan Sistem

3. Implementasi Algoritma AES

Pada tahap ini dilakukan implementasi algoritma AES pada aplikasi berbasis website. Proses enkripsi dilakukan saat pengguna mengunggah dokumen ke sistem, sedangkan proses dekripsi dilakukan ketika dokumen akan diakses oleh pengguna yang berwenang.

4. Pengujian Sistem

Pengujian sistem dilakukan untuk memastikan bahwa aplikasi yang dikembangkan berjalan sesuai dengan kebutuhan. Pengujian meliputi pengujian fungsional sistem untuk memastikan proses enkripsi dan dekripsi berjalan dengan benar, serta pengujian kinerja algoritma AES berdasarkan waktu proses enkripsi dan dekripsi terhadap beberapa ukuran file dokumen yang berbeda. Hasil pengujian digunakan untuk menganalisis efektivitas dan efisiensi algoritma AES dalam pengamanan dokumen berbasis website.

JURNAL SISTEM INFORMASI TGD
Volume 5, Nomor 1, Januari 2026, Hal 428-437
P-ISSN : 2828-1004 ; E-ISSN : 2828-2566
https://ojs.trigunadharma.ac.id/index.php/jsi

5. Analisa Hasil

Tahap ini bertujuan untuk menganalisis hasil pengujian sistem. Analisis dilakukan dengan membandingkan hasil enkripsi dan dekripsi, tingkat keberhasilan pengamanan dokumen, serta performa sistem dalam menangani file dengan ukuran yang bervariasi. Hasil analisis digunakan untuk menarik kesimpulan mengenai kelayakan algoritma AES sebagai solusi pengamanan dokumen pemerintahan berbasis website.

2.2 Teknik Pengumpulan Data

Teknik pengumpulan data dalam penelitian ini meliputi:

1. Studi Literatur, yaitu pengumpulan referensi yang berkaitan dengan kriptografi, algoritma AES, serta pengamanan dokumen berbasis website.
2. Observasi Sistem, yaitu pengamatan langsung terhadap kebutuhan pengelolaan dokumen pada lingkungan pemerintahan sebagai dasar perancangan sistem.

2.3 Penerapan Algoritma AES dalam Penelitian

Pada tahap ini dilakukan studi dan penerapan algoritma AES agar nantinya dapat diimplementasikan kepada sistem saat membangun sistem yang sudah dirancang. Berikut proses yang ada dalam algoritma AES dalam mengamankan sistem :

1. Ekspansi Kunci

Ekspansi Kunci dibutuhkan untuk proses enkripsi dan dekripsi pada algoritma Advanced Encryption Standart. Maksimal panjang kunci pada algoritma Advanced Encryption Standart 128 bit adalah 16 digit yang membutuhkan adalah 10 kunci ronde dalam ekspansi kunci. Kunci yang digunakan pada kasus ini adalah “KEL SITIREJO III”. Berikut adalah proses ekspansi kunci Advanced Encryption Standart :

a. Urutkan plaintext kunci kedalam blok berukuran 128 bit (16 kode ASCII), kemudian kunci diubah kedalam bentuk Hexadesimal :

K	E	L		S	I	T	I	R	E	J	O		I	I	I
4B	45	4C	20	53	49	54	49	52	45	4A	4F	20	49	49	49

b. Selanjutnya adalah mengubah kunci yang telah di ubah kedalam state dalam state 4 x 4 Sebagai berikut :

4B	53	52	20
45	49	49	49
4C	54	4A	49
20	49	4F	49

RoundKey 0

c. Melakukan fungsi RotWord, yaitu dengan menggeser setiap bit pada kolom 4 ke atas 1 kali menggunakan RoundKey ke-0 untuk menghasilkan RoundKey ke-1.

20	→	49
49		49
49		49
49		20

d. Melakukan subsitusi hasil dari RotWord dengan nilai yang ada pada tabel S-Box(SubBytes). Berikut hasil substitusi dengan tabel S-Box :

49	→	3B
49		3B
49		3B
20		B7

e. untuk mendapatkan kolom pertama dari RoundKey ke-1 adalah proses XOR antara kolom pertama dari RoundKey ke-0 dan hasil dari SubBytes di XOR-kan dengan Rcon

Tabel 1. Tabel Rcon

01	02	04	08	10	20	40	80	1B	3C
00	00	00	00	00	00	00	00	00	00
00	00	00	00	00	00	00	00	00	00
00	00	00	00	00	00	00	00	00	00

JURNAL SISTEM INFORMASI TGD
Volume 5, Nomor 1, Januari 2026, Hal 428-437
P-ISSN : 2828-1004 ; E-ISSN : 2828-2566
https://ojs.trigunadharma.ac.id/index.php/jsi

4B	XOR	XOR	3B	01	→	71	
45			3B	00		7E	
4C			3B	00		77	
20			B7	00		97	

f. Untuk mendapatkan nilai kolom selanjutnya dilakukan XOR antara kolom pertama (wi) dengan kolom kedua dari RoundKey ke-0, kemudian untuk mendapatkan kolom berikutnya lakukan proses seperti kolom kedua

53	XOR	71	→	22	
49		7E		37	
54		77		23	
49		97		DE	

Berikut hasil ekspansi kunci Roundkey 1 :

71	22	70	50
7E	37	72	3B
77	23	69	20
97	DE	91	D8

Untuk mendapatkan RoundKey ke-2 sampai dengan RoundKey ke-10, proses di atas diulang sebanyak 10 kali. Di bawah ini merupakan hasil eskpansi kunci dari setiap round yang akan digunakan untuk proses enkripsi dan dekripsi :

RoundKey ke-2			
91	B3	C3	93
C9	FE	8C	B7
16	35	5C	7C
C4	1A	8B	53

RoundKey ke-3			
3C	8F	4C	DF
D9	27	AB	1C
FB	CE	92	EE
18	02	89	DA

RoundKey ke-4			
A8	27	6B	B4
F1	D6	7D	61
AC	62	F0	1E
86	84	0D	D7

RoundKey ke-5			
57	70	1B	AF
83	55	28	49
A2	C0	30	2E
0B	8F	82	55

RoundKey ke-6			
4C	3C	27	88
B2	E7	CF	86
5E	9E	AE	80
72	FD	7F	2A

RoundKey ke-7			
48	74	53	DB
7F	98	57	D1
BB	25	8B	0B
B6	4B	34	1E

RoundKey ke-8			
F6	82	D1	0A
54	CC	9B	4A
C9	EC	67	6C
0F	44	70	6E

RoundKey ke-9			
3B	B9	68	62
04	C8	53	19
56	BA	DD	B1
68	2C	5C	32

RoundKey ke-10			
D9	60	08	6A
CC	04	57	4E
75	CF	12	A3
C2	EE	B2	80

2. Enkripsi

Proses enkripsi akan dilakukan dengan menggunakan plaintext “Fasilitas Publik” dengan proses enkripsi seperti berikut ini :

a. Plaintext diurutkan kedalam blok dan diubah kedalam bentuk bilangan hexadesimal.

F	A	S	I	L	I	T	A	S		P	U	B	L	I	K
46	41	53	49	4C	49	54	41	53	20	50	55	42	4C	49	4B

b. Plaintext yang di ubah ke hexadesimal yang telah disusun 16 byte pertama dibentuk kedalam state 4 x 4

46	4C	53	42
41	49	20	4C
53	54	50	49
49	41	55	4B

c. Selanjutnya proses AddRoundKey, pada proses ini XOR-kan plaintext dengan Roundkey ke-0

46	4C	53	42	XOR	4B	53	52	20	=	0D	1F	01	62
41	49	20	4C		45	49	45	49		04	00	65	05
53	54	50	49		4C	54	4A	49		1F	00	1A	00
49	41	55	4B		20	49	4F	49		69	08	1A	02

JURNAL SISTEM INFORMASI TGD
Volume 5, Nomor 1, Januari 2026, Hal 428-437
P-ISSN : 2828-1004 ; E-ISSN : 2828-2566
https://ojs.trigunadharma.ac.id/index.php/jsi

d. Hasil dari AddRoundKey di atas akan menjadi round ke-1 untuk di proses dengan 4 transformasi, yaitu SubBytes, ShiftRows, MixColumn, dan AddRoundKey.

e. Transformasi yang pertama yaitu SubBytes, pada tahap ini setiap byte akan ditukar dengan nilai pada tabel S-Box.

0D	1F	01	62
04	00	65	05
1F	00	1A	00
69	08	1A	02

→

D7	C0	7C	AA
F2	63	4D	6B
C0	63	A2	63
F9	30	A2	77

f. Transformasi berikutnya adalah ShiftRows, baris pertama tidak ada pergeseran, baris kedua dilakukan pergeseran 1 byte ke kiri, pada baris ketiga digeser 2 byte ke kiri dan pada baris keempat digeser 3 byte ke kiri.

D7	C0	7C	AA
F2	63	4D	6B
C0	63	A2	63
F9	30	A2	77

D7	C0	7C	AA
63	4D	6B	F2
A2	63	C0	63
77	F9	30	A2

g. Selanjutnya adalah proses MixColumns, dimana proses ini akan melakukan perkalian antara dot product dengan state hasil dari ShiftRows.

02	03	01	01
01	02	03	01
01	01	02	03
03	01	01	02

X

D7	C0	7C	AA
63	4D	6B	F2
A2	63	C0	63
77	F9	30	A2

Byte baris 1 kolom 1 ($S10,0$)
= ({02}{D7}) ⊕ ({03}{63}) ⊕ ({01}{A2}) ⊕ ({01}{77})
= ({10} {1101 0111}) ⊕ ({11} {0110 0011}) ⊕ 1010 0010 ⊕ 0111 0111
= (02).(D7)
= (10).(1101 0111)
= (x) . (x7 + x6 + x4 + x2 + x + 1)
= (x8 + x7 + x5 + x3 + x2 + x)
= (x4 + x3 + x + 1) + x7 + x5 + x3 + x2 + x
= x7 + x5 + x4 + x2 + 1
= 1011 0101
= (03).(63)
= (11).(0110 0011)
= (x + 1) . (x6 + x5 + x + 1)
= (x7 + x6 + x2 + x) + (x6 + x5 + x + 1)
= x7 + x5 + x2 + 1
= 1010 0101
= 10110101 ⊕ 10100101 ⊕ 10100010 ⊕ 01110111
= 11000101
= C5

h. Lakukan perkalian baris 1 kolom 2, baris 1 kolom 3, dan baris 1 kolom 4. Kemudian lakukan hingga mendapatkan hasil sebagai berikut :

C5	D6	B5	83
9B	06	C1	52
72	5B	DC	63
4D	9C	4F	2B

i. Transformasi akhir dari round ke-1 adalah AddRoundKey, hasil dari MixColumns akan di XOR-kan dengan RoundKey ke-1, seperti dibawah ini.

C5	D6	B5	83
9B	06	C1	52
72	5B	DC	63
4D	9C	4F	2B

⊕

71	22	70	50
7E	37	72	3B
77	23	69	20
97	DE	91	D8

=

B4	F4	C5	D3
E5	31	B3	69
05	78	B5	43
DA	42	DE	F3

JURNAL SISTEM INFORMASI TGD
Volume 5, Nomor 1, Januari 2026, Hal 428-437
P-ISSN : 2828-1004 ; E-ISSN : 2828-2566
https://ojs.trigunadharma.ac.id/index.php/jsi

j. Proses diatas akan diulangi untuk round ke-2 sampai dengan round ke-10. Namun pada round ke-10 transformasi MixColumns tidak lagi dilakukan. Berikut hasil transformasi proses enkripsi round ke-2 sampai dengan round ke-10. Berikut hasil ronde ke-10 :

AddRoundKey			
63	B4	EF	02
FB	86	AE	A7
77	E4	85	03
DC	7C	43	40

Hasil dari proses enkripsi yaitu : 63FB77DCB486E47CEFA E854302A70340

3. Dekripsi

Proses ini dilakukan untuk mengembalikan record yang telah dienkripsi menjadi plaintext kembali, Transformasi deskripsi pada algoritma advanced encryption standart adalah InvSubBytes, InvShiftRows, InvMixColumns, dan AddRoundKey. Berikut ini adalah proses dekripsi dari chipertext "63FB77DCB486E47CEFA E854302A70340"

a. Pertama-tama, melakukan proses XOR antara chipertext dengan RoundKey ke-10

63	B4	EF	02
FB	86	AE	A7
77	E4	85	03
DC	7C	43	40

XOR =

D9	60	08	6A
CC	04	57	4E
75	CF	12	A3
C2	EE	B2	80

BA	D4	E7	68
37	82	F9	E9
02	2B	97	A0
1E	92	F1	C0

b. Selanjutnya, Pada round ke-1 sampai dengan round ke-9 proses dekripsi dilakukan transformasi InvShiftRows, InvSubBytes, InvMixColumns, dan AddRoundkey.

c. Lakukan proses InvShiftRows

BA	D4	E7	68
37	82	F9	E9
02	2B	97	A0
1E	92	F1	C0

→

BA	D4	E7	68
E9	37	82	F9
97	A0	02	2B
92	F1	C0	1E

d. Kemudian, lakukan proses InvSubBytes. Untuk S-Box InvSubBytes berbeda dengan S-Box SubBytes karena telah dilakukan invers namun, cara kerjanya sama.

BA	D4	E7	68
E9	37	82	F9
97	A0	02	2B
92	F1	C0	1E

→

C0	19	B0	F7
EB	B2	11	69
85	47	6A	0B
74	2B	1F	E9

e. Lakukan operasi XOR antara InvSubBytes dengan RoundKey ke-9 untuk transformasi AddRoundKey.

C0	19	B0	F7
EB	B2	11	69
85	47	6A	0B
74	2B	1F	E9

⊕

3B	B9	68	62
04	C8	53	19
56	BA	DD	B1
68	2C	5C	32

=

FB	A0	D8	95
EF	7A	42	70
D3	FD	B7	BA
1C	07	43	DB

f. Selanjutnya, melakukan proses Transformasi InvMixColumns antara hasil AddRoundKey dengan dot product dengan mengikuti aturan irreducible polynomial.

0E	0B	0D	09
09	0E	0B	0D
0D	09	0E	0B
0B	0D	09	0E

X

FB	A0	D8	95
EF	7A	42	70
D3	FD	B7	BA
1C	07	43	DB

(0E).(FB)
= (1110).(1111 1011)
= (x3 + x2 +x) (x7 + x6 + x5 + x4 + x3 + x + 1)
= (x10 + x9 + x8 + x7 + x6 + x4 + x3) + (x9 + x8 + x7 + x6+ x5 + x3 + x2) + (x8 + x7+ x6 + x5+ x4 + x2 + x)
= x10 + x8 + x7 + x6 + x
= (x2 . x8) + x8 + x7 + x6 + x

JURNAL SISTEM INFORMASI TGD
Volume 5, Nomor 1, Januari 2026, Hal 428-437
P-ISSN : 2828-1004 ; E-ISSN : 2828-2566
https://ojs.trigunadharma.ac.id/index.php/jsi

= x2 (x4 + x3 + x + 1) + (x4 + x3 + x + 1) + x7 + x6 + x
= x6 + x5 + x3 + x2 + x4 + x3 + x + 1 + x7 + x6 + x
= x7 + x5 + x4 + x2 + 1
= 1011 0101
= B5

Lakukan perkalian baris dikali kolom hingga selesai untuk baris pertama dan kolom pertama. Setelah proses tersebut, masing-masing hasil di-XOR, seperti berikut ini :
= 10110101 ⊕ 00010011 ⊕ 01110000 ⊕ 11111100
= 00101010
= 2A (Hasil baris pertama kolom pertama)

Lalu lakukan proses yang sama seperti pada baris 1 kolom 1. Di bawah ini adalah hasil dalam bentuk *state* 4x4

2A	5B	63	30
2F	BB	84	AD
AF	46	D0	0C
71	86	59	15

g. Lakukan proses dekripsi dan ulangi hingga ronde ke 10 sampai didapatkan hasil perhitungan pada ronde ke 10 sebagai berikut :

AddRoundKey			
46	4C	53	42
41	49	20	4C
53	54	50	49
49	41	55	4B

Maka, didapat hasil dekripsi : 464153494C4954415320505542 4C494B

3. HASIL DAN PEMBAHASAN

Hasil dari penelitian ini berupa sebuah aplikasi pengamanan dokumen pemerintahan berbasis website yang menerapkan algoritma Advanced Encryption Standard (AES) sebagai mekanisme enkripsi dan dekripsi file dokumen. Sistem yang dikembangkan menyediakan fitur unggah dokumen, proses enkripsi otomatis sebelum penyimpanan, serta proses dekripsi saat dokumen diakses oleh pengguna yang memiliki hak akses. Dengan penerapan algoritma AES, dokumen yang tersimpan dalam sistem tidak dapat dibaca secara langsung tanpa melalui proses dekripsi menggunakan kunci yang sesuai.

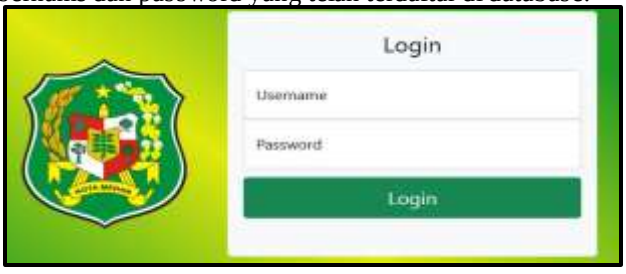
Implementasi algoritma AES pada sistem berhasil mengubah file dokumen asli menjadi bentuk terenkripsi (ciphertext) sehingga isi dokumen tidak dapat dikenali. File hasil enkripsi memiliki format dan struktur data yang berbeda dengan file asli, menandakan bahwa proses pengamanan data telah berjalan dengan baik. Proses dekripsi juga berhasil mengembalikan file terenkripsi ke bentuk semula tanpa perubahan isi dokumen, yang menunjukkan bahwa algoritma AES dapat menjaga integritas data.

3.1 Pengujian Aplikasi

Berikut hasil dari pengujian aplikasi pengamanan dokumen pemerintahan berbasis website yang menerapkan algoritma Advanced Encryption Standard (AES) sebagai mekanisme enkripsi dan dekripsi file dokumen pada pemerintahan yang ada di kelurahan Siti Rejo III :

1. Form Login

Form login merupakan halaman yang digunakan oleh admin untuk masuk ke dalam aplikasi. Form login akan melakukan validasi terhadap username dan password yang telah terdaftar di database.



Gambar 2. Form Login

JURNAL SISTEM INFORMASI TGD
Volume 5, Nomor 1, Januari 2026, Hal 428-437
P-ISSN : 2828-1004 ; E-ISSN : 2828-2566
https://ojs.trigunadharma.ac.id/index.php/jsi

2. Menu Utama

Menu Utama (home) dari aplikasi yang dirancang sebagai halaman paling awal dari sistem :

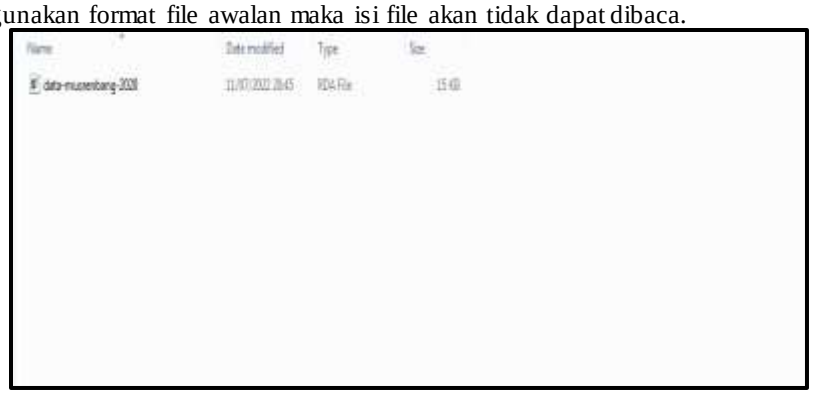
Gambar 3. Menu Utama

3. Form Enkripsi

Enkripsi dilakukan dengan menekan tombol Browse untuk memilih file dari windows explorer, kemudian memasuukan password dan deskripsi dari file tersebut.

Gambar 4. Enkripsi File

Kemudian, setelah diklik tombol enkripsi file, maka file tersebut akan berubah format menjadi .RDA serta apabila dibuka menggunakan format file awalan maka isi file akan tidak dapat dibaca.

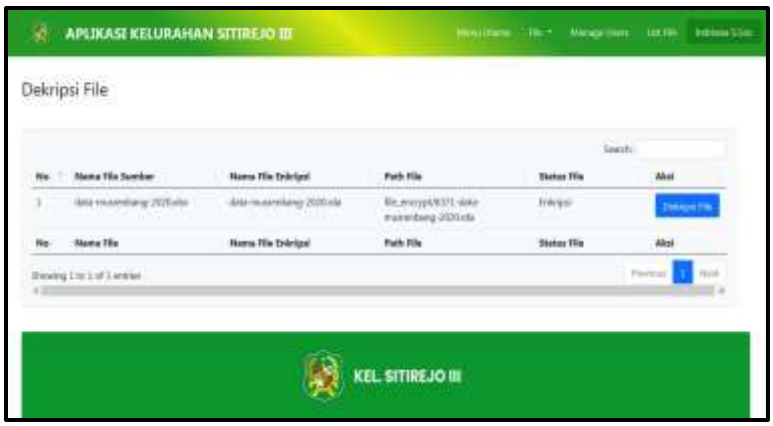


Gambar 5. Hasil Enkripsi File

4. Form Dekripsi

Sebelum mendekripsi file, pada tampilan menu dekripsi terlihat file yang sebelumnya sudah dienkripsi. File-file tersebut dapat dipilih untuk mendekripsinya dengan menekan tombol dekripsi file

JURNAL SISTEM INFORMASI TGD
Volume 5, Nomor 1, Januari 2026, Hal 428-437
P-ISSN : 2828-1004 ; E-ISSN : 2828-2566
https://ojs.trigunadharma.ac.id/index.php/jsi

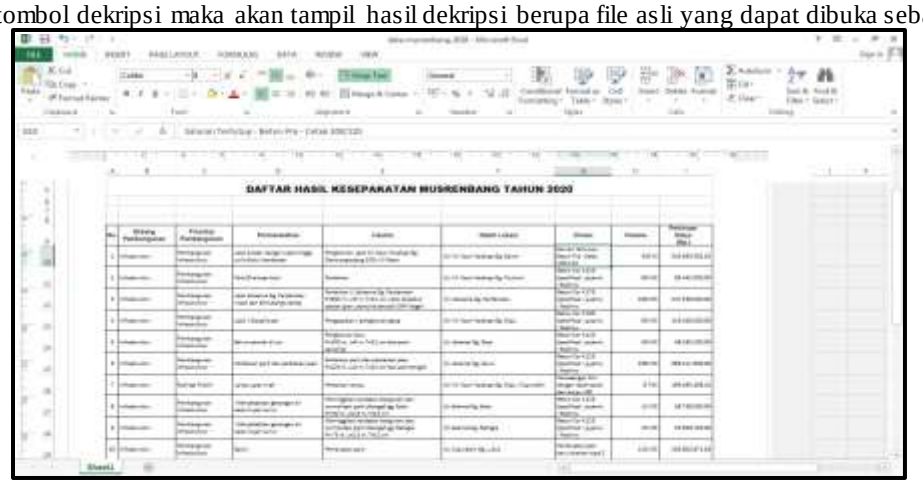


Gambar 6. Tampilan Menu Dekripsi File

Saat, tombol dekripsi file dipilih, makan akan tampil form dekripsi sebagai berikut :

Gambar 7. Dekripsi File

Pada form ini dilakukan dekripsi file dengan cara memasukkan password yang digunakan saat mengenkripsi file, kemudian tekan tombol dekripsi maka akan tampil hasil dekripsi berupa file asli yang dapat dibuka sebagai berikut :



Gambar 8. Hasil Dekripsi File

Hasil penelitian ini memberikan implikasi bahwa sistem pengamanan dokumen pemerintahan berbasis website dengan menggunakan algoritma AES dapat dijadikan sebagai alternatif solusi keamanan informasi di lingkungan pemerintahan. Sistem yang dikembangkan dapat membantu melindungi dokumen penting dari ancaman kebocoran data serta meningkatkan kepercayaan terhadap pemanfaatan teknologi informasi dalam pengelolaan dokumen penting yang wajib diamankan di lingkungan pemerintahan.

4. KESIMPULAN

Berdasarkan hasil implementasi dan pengujian yang telah dilakukan, dapat disimpulkan bahwa penerapan algoritma AES pada aplikasi pengamanan dokumen berbasis website mampu meningkatkan tingkat keamanan data dokumen. Hasil penelitian ini sejalan dengan penelitian-penelitian sebelumnya yang menyatakan bahwa algoritma AES efektif dalam melindungi data sensitif pada sistem berbasis web.

Keberhasilan proses enkripsi dan dekripsi menunjukkan bahwa algoritma AES tidak hanya mampu menjaga kerahasiaan dokumen, tetapi juga mempertahankan integritas data. Selain itu, hasil pengujian kinerja menunjukkan bahwa penggunaan algoritma AES tidak menyebabkan penurunan performa sistem yang signifikan, sehingga tetap sesuai untuk diterapkan pada lingkungan pemerintahan yang membutuhkan akses data secara cepat dan aman.

Jika dibandingkan dengan penelitian sebelumnya yang berfokus pada pengamanan dokumen umum atau sistem non-pemerintahan, penelitian ini memberikan kontribusi tambahan dengan menerapkan algoritma AES secara khusus pada konteks dokumen pemerintahan berbasis website. Hal ini menunjukkan bahwa algoritma AES dapat diadaptasi dan diimplementasikan secara efektif dalam mendukung pengembangan sistem e-government yang aman.

DAFTAR PUSTAKA

[1] Y. Jordan, E. L. Anwar, R. Habibi, and N. Riza, "UNTUK MENGAMANKAN FILE DOKUMEN," vol. 16, no. 2, 2022.
[2] M. L. Assidiq, F. Mahardika, and D. Santika, "Implementasi Algoritma Kriptografi AES dan SHA-3 Dalam Mengamankan Data Sensitif Pengguna Pada Website Transaksi," vol. 4, no. 1, pp. 44–52, 2024.
[3] A. H. Nasrullah, "Secure Web-Based File Encryption Using AES-128," vol. 6, no. 2, pp. 146–155, 2025.
[4] A. E. Standard, K. Dokumen, and B. B. Testing, "1,2 1* , 2," no. November 2018, pp. 1044–1052, 2024.
[5] H. Shadzily and B. Sujatmiko, "ANALISIS TINGKAT KEAMANAN FILE DOKUMEN MENGGUNAKAN ALGORITMA ADVANCED ENCRYPTION STANDARD (AES) Fakultas Teknologi Informasi , Universitas Hasyim Asy ' ari Jombang Jawa Timur Indonesia DOCUMENT FILE SECURITY LEVEL ANALYSIS USING ADVANCED ENCRYPTION STANDARD (AES) ALGORITHM," vol. 2025, no. September, pp. 37–44, 2025, doi: 10.33752/inovate.v10i1.9251.
[6] M. A. Maryo, B. W. Widagdo, P. Studi, T. Informatika, and U. Pamulang, "IMPLEMENTASI KRIPTOGRAFI ADVANCED ENCRYPTION STANDARD (AES-128) UNTUK PENGAMANAN FILE SOAL BERBASIS WEB PADA SMP GUNUNG JATI KOTA TANGERANG," vol. 3, no. 2, pp. 26–31, 2025.
[7] M. A. Hasan, "Aplikasi Keamanan Data Berbasis Web Menggunakan Algoritma AES 128 Untuk Enkripsi Dan Dekripsi Data," vol. 2, no. 2, 2022.
[8] S. F. Manullang, "P d f d m a a e s m c b c," vol. 17, no. 1, pp. 53–67, 2023.
[9] G. Divva, M. Zulma, H. B. Seta, and T. Yuniati, "Implementasi Algoritma AES Dan Bcrypt untuk Pengamanan File Dokumen," vol. 4221, pp. 163–176, 2022.
[10] H. Indriyawati, T. Winarti, V. Vydia, and A. Encryption, "Web-based Secure Degree Certificate Legalization System Using Advanced Encryption Standard Algorithm," vol. 7, no. 1, pp. 17–21, 2024.
[11] F. A. Naimnule, F. A. L. Hanoe, M. N. Banusu, and M. O. Mano, "Implementation of AES Encryption for Data Security on Web-Based Information Systems in Fafinesu A Village," vol. 4, no. 3, pp. 122–130, 2025.
[12] S. K. Waybhase, "Data Security using Advanced Encryption Standard (AES)," vol. 11, no. 06, pp. 630–632, 2022.
[13] D. Irwanto, "File Encryption and Decryption Using Algorithm Aes-128 Bit Based Website," vol. 4, no. April, pp. 670–677, 2024.
[14] F. Aditya and M. A. Romli, "TIN : Terapan Informatika Nusantara Implementasi Metode Kriptografi Advanced Encryption Standard 256 Bit Berbasis Web dan Mobile Pada Pengamanan Dokumen Notaris TIN : Terapan Informatika Nusantara," vol. 6, no. 6, pp. 707–714, 2025, doi: 10.47065/tin.v6i6.8637.