JURNAL TIMES
TECHNOLOGY INFORMATICS & COMPUTER SYSTEM

Volume XIII No 2, Desember 2024
*p*ISSN : 2337 – 3601
*e*ISSN : 2549 – 015X

Tersedia *online* di http://ejournal.stmik-time.ac.id

ALGORITMA AES UNTUK KEAMANAN DATA DIGITAL BERBASIS *WEB* DI KANTOR DESA AMAN DAMAI

Mira Tania[1)], Tomy Satria Alasi[2)], Riandy Yap[3)]
Teknik Informatika
STMIK Methodist Binjai
Jl. Jenderal Gatot Subroto, Binjai Barat, 20716
email: ainatarim@gmail.com[1)], tomysatriaalasi@live.com[2)], riandy.yap89@stmikmethodistbinjai.ac.id[3)]

Abstrak

Seiring berkembangnya teknologi informasi, keamanan data digital menjadi aspek penting dalam upaya melindungi informasi yang sifatnya sensitif. Penelitian ini bertujuan untuk untuk memahami bagaimana algoritma *Advanced Encryption Standard* (AES) 128 bit dapat digunakan untuk melindungi data digital di Kantor Desa Aman Damai, serta merancang dan mengembangkan aplikasi berbasis *web* yang dapat mengamankan data tersebut menggunakan algoritma ini. AES 128 bit merupakan algoritma enkripsi simetris yang dikenal efektif dalam menjaga data agar tidak diakses secara ilegal. Metode penelitian yang digunakan melibatkan analisis teknis dari algoritma AES 128 bit, termasuk enkripsi dan dekripsi. Penelitian ini mengungkap bahwa penerapan algoritma AES 128 bit bisa meningkatkan keamanan data digital dengan baik, mampu melindungi informasi seperti dokumen surat penting. Penelitian ini memberikan kontribusi terhadap pemahaman tentang efektivitas dan penerapan algoritma AES 128 bit dalam aplikasi berbasis *web* di Kantor Desa Aman Damai.

Kata Kunci: Algoritma AES 128 bit, Keamanan Data Digital, Enkripsi, Dekripsi, Aplikasi Berbasis *Web*

1. Pendahuluan

Dalam era digital saat ini, teknologi informasi telah merambah ke berbagai sektor, termasuk kantor pemerintahan seperti kantor desa. Sistem informasi desa yang diterapkan di Kantor Desa Aman Damai mengelola berbagai data digital, seperti surat keterangan, surat perizinan, surat perjanjian dan sebagainya. Keamanan data digital di desa perlu dipastikan untuk mencegah penyalahgunaan. Sangat penting untuk melindungi data digital agar informasi tidak disalahgunakan, terutama karena Kantor Desa Aman Damai masih menyimpan data di komputer atau flashdisk tanpa aplikasi pengaman tambahan. Risiko kebocoran informasi seperti pencurian fisik komputer, penyalahgunaan data oleh pegawai, dan kebocoran data akibat kelalaian dapat terjadi jika data tidak dilindungi dengan baik. Kriptografi, yang melibatkan proses enkripsi untuk mengubah pesan menjadi bentuk yang tidak dapat dipahami adalah salah satu solusi untuk melindungi data digital. Algoritma kriptografi yang umum digunakan adalah Advanced Encryption Standard (AES).

Dalam penelitian ini, penulis memilih untuk menggunakan algoritma AES dengan panjang kunci 128 bit yang diharapkan dapat meningkatkan keamanan data digital di Kantor Desa Aman Damai. Dengan menerapkan algoritma AES 128 bit, penelitian ini bertujuan memberikan pemahaman yang lebih baik tentang teknologi enkripsi untuk melindungi data digital dari pihak yang tidak berwenang. Penelitian ini mengidentifikasi masalah utama di Kantor Desa Aman Damai, yaitu belum adanya aplikasi pengamanan data digital. Oleh karena itu, penerapan algoritma AES 128 bit diperlukan untuk melindungi data tersebut. Batasan penelitian ini meliputi penerapan enkripsi menggunakan AES 128 bit untuk file dengan format doc, docx, txt, pdf, xls, dan xlsx dengan ukuran maksimal 6 MB serta hasil enkripsi yang berupa file dengan format *.enc. Tujuan penelitian ini adalah untuk memahami bagaimana algoritma AES 128 bit dapat digunakan dalam melindungi data digital di Kantor Desa Aman Damai, serta mengembangkan aplikasi berbasis web yang dapat mengamankan data digital dengan menggunakan algoritma AES 128 bit. Penelitian ini diharapkan dapat memberikan manfaat bagi Kantor Desa Aman Damai, yaitu meningkatkan keamanan data digital dan melindunginya dari akses yang tidak sah serta manipulasi.

2. Landasan Teori

Keamanan Data Digital

Keamanan data Digital mencakup langkah-langkah untuk melindungi informasi digital dari akses ilegal, kerusakan, perubahan, pencurian, atau pengungkapan yang tidak sah. Proses ini melibatkan berbagai teknik, mulai dari perlindungan perangkat keras fisik (seperti perangkat penyimpanan), keamanan perangkat lunak, kontrol administratif dan akses, kebijakan organisasi, serta metode keamanan lainnya [1].

Data dapat dimanfaatkan oleh pihak yang tidak berwenang untuk tujuan yang merugikan, misalnya pencurian identitas, penipuan, atau tindak kejahatan lainnya. Oleh karena itu, diperlukan sistem keamanan yang dapat melindungi data dari risiko-risiko tersebut [2].

Kriptografi

Kriptografi berasal dari kata Yunani, "*crypto*" yang berarti rahasia dan "*graphia*" yang berarti tulisan [3]. Selain itu, menurut Munir dalam [4], kriptografi adalah bidang ilmu yang berfokus pada teknik-teknik perhitungan untuk menjaga keamanan informasi, termasuk kerahasiaan, integritas data, serta autentikasi. Berdasarkan definisi tersebut, maka dapat disimpulkan bahwa kriptografi adalah bidang ilmu yang melibatkan berbagai teknik dan metode untuk memastikan informasi tetap terlindungi dari akses, perubahan, atau pemalsuan yang dilakukan oleh pihak tidak berwenang

Kunci Simetri

Dalam dunia kriptografi, proses enkripsi dan dekripsi bergantung pada penggunaan kunci simetri, yang berperan sebagai kunci utama untuk menyandikan dan membuka pesan. Kunci ini berfungsi baik dalam proses enkripsi maupun dekripsi.

Kunci simetri sendiri adalah jenis kunci yang sama digunakan untuk mengenkripsi dan mendekripsi data. Dalam algoritma kriptografi berbasis kunci simetri, pihak yang melakukan enkripsi dan pihak yang melakukan dekripsi harus memiliki akses ke kunci yang sama. Oleh karena itu, keamanan dari metode ini sangat tergantung pada kerahasiaan dan perlindungan terhadap kunci tersebut [5].

***Algoritma Advanced Encryption Standard* (AES)**

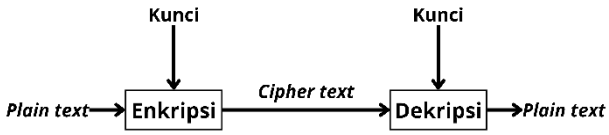
Algoritma *Advanced Encryption Standard* (AES) merupakan algoritma *cipher* yang digunakan untuk melindungi informasi yang sifatnya rahasia. Sejak tahun 2001, AES mengganti peran algoritma *Data Encryption Standard* (DES) yang sudah usang dan rentan terhadap serangan peretasan. AES menggunakan berbagai ukuran kunci, yakni 128 bit, 192 bit, dan 256 bit, yang mempengaruhi jumlah putaran dalam proses enkripsi dan dekripsi [6]. Dalam penelitian ini, digunakan AES 128 bit untuk melindungi data digital.

3. Metode Penelitian

Penelitian ini menggunakan metode analisis teknis untuk memahami dan mengevaluasi penerapan algoritma *Advanced Encryption Standard* (AES) 128 bit. Analisis ini mencakup proses enkripsi dan dekripsi, yang merupakan langkah-langkah penting dalam memastikan keamanan data digital.

Proses Enkripsi dan Dekripsi

Proses enkripsi dan dekripsi dapat dianggap sebagai inti dari upaya perlindungan data. Proses ini melibatkan perubahan data asli yang disebut *plaintext* (pesan dalam bentuk biasa) menjadi *ciphertext* (pesan yang sudah disandikan) sehingga pihak yang tidak berwenang tidak dapat membaca atau memahami isinya, serta untuk menjaga kerahasiaan data tersebut. Proses mengubah *plaintext* menjadi *ciphertext* disebut dengan istilah enkripsi (*encryption*) atau *enciphering*. Sebaliknya, proses untuk mengubah *ciphertext* kembali ke bentuk *plaintext* semula disebut dekripsi (*decryption*) atau *deciphering*. Ilustrasi proses enkripsi dan dekripsi dapat dilihat pada gambar berikut.



Gambar 1. Ilustrasi Proses Enkripsi dan Dekripsi

Pengamanan Data dengan AES 128 Bit

Dalam bagian ini, akan dibuat contoh perhitungan manual untuk enkripsi dan dekripsi AES 128 bit. Untuk memperoleh hasil enkripsi dan dekripsi dari suatu data, algoritma ini memerlukan beberapa tahap perhitungan manual. Berikut adalah contoh perhitungan manual enkripsi dan dekripsi AES 128 bit.

1. Contoh Data

   Plaintext : MIRATANIAMIRATAN

   Cipher key : KRIPTOGRAFIAESKU

Plaintext

M	I	R	A
T	A	N	I

Heksadesimal

4D	49	52	41
54	41	4E	49

A	M	I	R
A	T	A	N

41	4D	49	52
41	54	41	4E

Cipher Key

K	R	I	P
T	O	G	R
A	F	I	A
E	S	K	U

Heksadesimal

4B	52	49	50
54	4F	47	52
41	46	49	41
45	53	4B	55

2. *Key Expansion* (Ekspansi Kunci)

Sebanyak 10 kunci dihasilkan untuk mendukung proses enkripsi yang terdiri dari 10 *round*. Setiap *round* melibatkan langkah *addroundkey*, sehingga dibutuhkan satu kunci per *round*, dengan total 10 kunci yang digunakan sepanjang proses enkripsi. Pada proses pembangkitan kunci diperlukan tabel *S-Box* dan *Rcon*.

Tabel 1. Tabel S-Box

	x0	x1	x2	x3	x4	x5	x6	x7	x8	x9	xa	xb	xc	xd	xe	xf
0x	63	7c	77	7b	f2	6b	6f	c5	30	1	67	2b	fe	d7	ab	76
1x	ca	82	c9	7d	fa	59	47	f0	ad	d4	a2	af	9c	a4	72	c0
2x	b7	fd	93	26	36	3f	f7	cc	34	a5	e5	f1	71	d8	31	15
3x	4	c7	23	c3	18	96	5	9a	7	12	80	e2	eb	27	b2	75
4x	9	83	2c	1a	1b	6e	5a	a0	52	3b	d6	b3	29	e3	2f	84
5x	53	d1	0	ed	20	fc	b1	5b	6a	cb	be	39	4a	4c	58	cf
6x	d0	ef	aa	fb	43	4d	33	85	45	f9	2	7f	50	3c	9f	a8
7x	51	a3	40	8f	92	9d	38	f5	bc	b6	da	21	10	ff	f3	d2
8x	cd	0c	13	ec	5f	97	44	17	c4	a7	7e	3d	64	5d	19	73
9x	60	81	4f	dc	22	2a	90	88	46	ee	b8	14	de	5e	0b	db
ax	e0	32	3a	0a	49	6	24	5c	c2	d3	ac	62	91	95	e4	79
bx	e7	c8	37	6d	8d	d5	4e	a9	6c	56	f4	ea	65	7a	ae	8
cx	ba	78	25	2e	1c	a6	b4	c6	e8	dd	74	1f	4b	bd	8b	8a
dx	70	3e	b5	66	48	3	f6	0e	61	35	57	b9	86	c1	1d	9e
ex	e1	f8	98	11	69	d9	8e	94	9b	1e	87	e9	ce	55	28	df
fx	8c	a1	89	0d	bf	e6	42	68	41	99	2d	0f	b0	54	bb	16

Tabel 2. Tabel *Rcon*

Round	**1**	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**	**10**
Rcon[]	01	02	04	08	10	20	40	80	1b	36
	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

w[0] =	4B	52	49	50	
w[1] =	54	4F	47	52	
w[2] =	41	46	49	41	
w[3] =	45	53	4B	55	

g(w[3]) =	53	4B	55	45	(Geser kiri 1 kolom / *RotWord*)
	ED	B3	FC	6E	(Substitusi AES *S-Box*)
	1	0	0	0	(*Rcon*)
	237	179	252	110	(Substitusi AES *S-Box* dalam desimal)
	1	0	0	0	(*Rcon* dalam desimal)
	236	179	252	110	(Substitusi AES *S-Box* XOR *Rcon*)

w[4] =	4B	52	49	50	w[0]
	EC	B3	FC	6E	g(w[3])

75	82	73	80	(w[0] dalam desimal)
236	179	252	110	(g(w[3]) dalam desimal)
167	225	181	62	w[0] XOR g(w[3])

w[5] =

A7	E1	B5	3E	w[4]
54	4F	47	52	w[1]
167	225	181	62	(w[4] dalam desimal)
84	79	71	82	(w[1] dalam desimal)
243	174	242	108	w[4] XOR w[1]

w[6] =

F3	AE	F2	6C	w[5]
41	46	49	41	w[2]
243	174	242	108	(w[5] dalam desimal)
65	70	73	65	(w[2] dalam desimal)
178	232	187	45	w[5] XOR w[2]

w[7] =

B2	E8	BB	2D	w[6]
45	53	4B	55	w[3]
178	232	187	45	(w[6] dalam desimal)
69	83	75	85	(w[3] dalam desimal)
247	187	240	120	w[6] XOR w[3]

3. Kunci (W)

R0	4B	52	49	50	54	4F	47	52	41	46	49	41	45	53	4B	55
R1	A7	E1	B5	3E	F3	AE	F2	6C	B2	E8	BB	2D	F7	BB	F0	78
R2	59	AF	7B	83	40	BD	E4	CE	6F	97	4A	B3	74	89	DD	F9
R3	FA	6E	E2	11	BA	D3	06	DF	D5	44	4C	6C	A1	CD	91	95
R4	4F	EF	C8	23	F5	3C	CE	FC	20	78	82	90	81	B5	13	05
R5	8A	92	A3	2F	7F	AE	6D	D3	5F	D6	EF	43	DE	63	FC	46
R6	51	22	F9	32	2E	8C	94	E1	71	5A	7B	A2	AF	39	87	E4
R7	03	35	90	4B	2D	B9	04	AA	5C	E3	7F	08	F3	DA	F8	EC
R8	D4	74	5E	46	F9	CD	5A	EC	A5	2E	25	E4	56	F4	DD	08
R9	70	B5	6E	F7	89	78	34	1B	2C	56	11	FF	7A	A2	CC	F7
R10	7C	FE	06	2D	F5	86	32	36	D9	D0	23	C9	A3	72	EF	3E

4. Proses Enkripsi

Penelitian ini menggunakan algoritma AES 128 bit dengan jumlah *round* (putaran) sebanyak 10 kali. Proses enkripsi dalam algoritma ini terdiri dari 4 operasi yaitu *SubBytes*, *ShiftRows*, *MixColumns* dan *AddRoundKey* pada *round* 1 hingga *round* 9. Pada *round* 10, tidak dilakukan lagi proses *MixColumns*.

- *Initial Round / AddRoundKey* (melakukan operasi XOR pada *plaintext* (P) dengan *cipher key* (W) dan hasil dari operasi ini akan digunakan untuk proses enkripsi di *round* 1).
- *Round* 0 : 06 00 00 04 1B OE OB 07 1B 09 00 0A 11 1B 13 1B
- *Round* 1 :
  - *SubBytes* (menukar isi dari *byte* hasil operasi XOR pada *initial round* sebelumnya dengan menggunakan tabel *S-Box*) :
    6F 63 63 F2 AF AB 2B C5 AF 01 63 67 82 AF 7D AF
  - *ShiftRows* (tahapan pergeseran blok berdasarkan baris dari hasil *SubBytes* sebelumnya) :
    6F 63 63 F2 AB 2B C5 AF 63 67 AF 01 AF 82 AF 7D
  - *MixColumns* (setiap kolom dari hasil *ShiftRows* sebelumnya dikalikan dengan matriks AES) :
    F4 DD 32 7A A9 DA 78 96 CF CC 6D 33 43 A7 35 DC
  - *AddRoundKey* (mengombinasikan hasil *MixColumns* dan *round key* dengan hubungan XOR) :
    53 2E 80 8D 48 74 90 2D 7A 3E D6 C3 7D CB 18 A4
- *Round* 10 :
  - *SubBytes* : F3 06 94 69 3F 2B B8 2E 4A D5 0E 14 BB 86 35 37
  - *ShiftRows* : F3 6 94 69 2B B8 2E 3F E 14 4A D5 37 BB 86 35
  - *AddRoundKey* : 8F F3 4D CA D5 3E FE 4D 8 26 69 3A 1A 8D 4F B
- Hasil Enkripsi : 8F F3 4D CA D5 3E FE 4D 8 26 69 3A 1A 8D 4F B

5. Proses Dekripsi

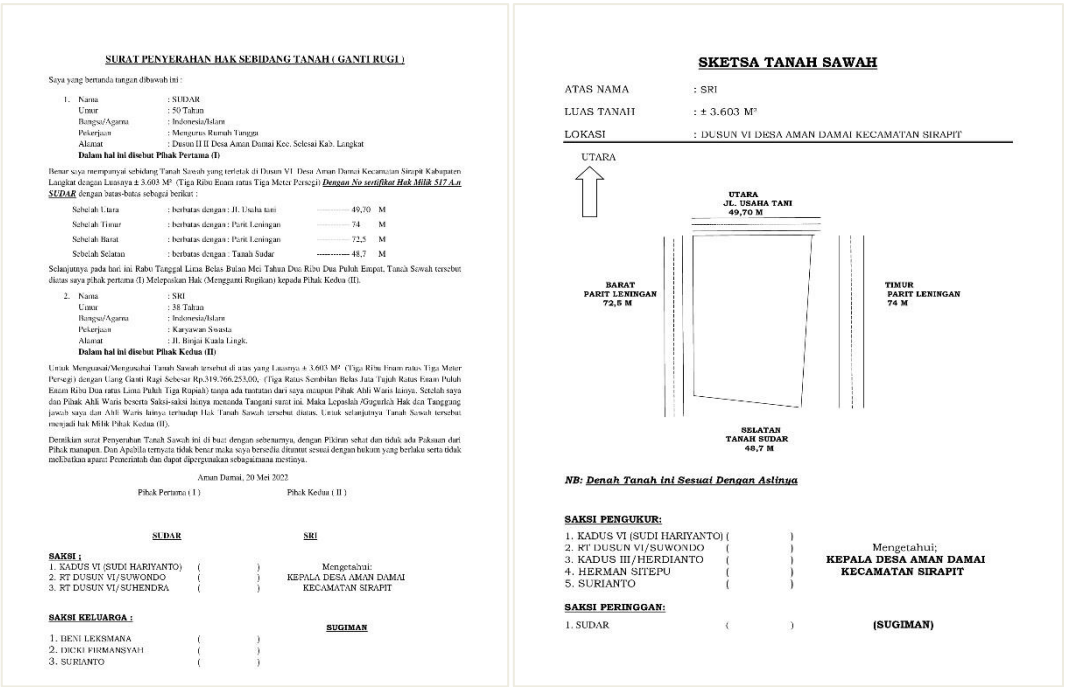
Proses dekripsi ini terdiri dari 4 operasi yaitu *InvShiftRows, InvSubBytes, InvAddRoundKey* dan *InvMixColumns* pada *round* 1 hingga *round* 9. Pada *round* 10, tidak dilakukan lagi proses *InvMixColumns.*

- *InvAddRoundKey* (melakukan operasi XOR pada *ciphertext* menggunakan *round key* ke-10) :
  F3, 6, 94, 69, 2B, B8, 2E, 3F, 0E, 14, 4A, D5, 37, BB, 86, 35
- *Round* 1 :
  - *InvShiftRows* (melakukan pergeseran bit ke kanan pada setiap blok baris hasil operasi XOR *InvAddRoundKey*) :
    F3, 6, 94, 69, 3F, 2B, B8, 2E, 4A, D5, 0E, 14, BB, 86, 35, 37
  - *InvSubBytes* (setiap elemen dalam *state* yang diperoleh dari *InvShiftRows* akan dipetakan menggunakan tabel *Inverse S-Box*) :
    7E, A5, E7, E4, 25, 0B, 9A, C3, 5C, B5, D7, 9B, FE, DC, D9, B2
  - *InvAddRoundKey* (mengombinasikan hasil *InvSubBytes* dan *round key* dengan hubungan XOR) :
    0E, 2C, CB, 9E, 90, 73, CC, 61, 32, 81, C6, 57, 09, C7, 26, 45
  - *InvMixColumns* (setiap kolom dari hasil *InvAddRoundKey* dikalikan dengan matriks AES) :
    23, C1, 6F, B6, 67, BB, C3, 59, 75, 5E, B7, BE, AF, 3D, FC, BC
- *Round* 10 :
  - *InvShiftRows* : 36 4C E8 F4 81 3C AA D2 EF D9 38 6 2C A2 B2 BA
  - *InvSubBytes* : 7D 64 77 75 7C 74 75 60 65 7C 78 78 75 28 62 79
  - *InvAddRoundKey* : 4D 49 52 41 54 41 4E 49 41 4D 49 52 41 54 41 4E

Hasil Dekripsi : 4D 49 52 41 54 41 4E 49 41 4D 49 52 41 54 41 4E

Bahan atau Data

Pada aplikasi berbasis *web* ini, sampel data digital yang digunakan berupa *file* dokumen *word*, yakni surat penyerahan hak atas sebidang tanah. Surat ini berisi informasi penting seperti penyerahan hak tanah, nomor sertifikat hak milik, harga ganti rugi, pengesahan, saksi dan sketsa tanah. Sampel data digital yang penulis peroleh dari Kantor Desa Aman Damai dapat diamati pada gambar berikut.



SURAT PENYERAHAN HAK SEBIDANG TANAH (GANTI RUGI)

Saya yang bertanda tangan dibawah ini :

1. Nama : SUDAR
   Umur : 50 Tahun
   Bangsa/Agama : Indonesia/Islam
   Pekerjaan : Mengurus Rumah Tangga
   Alamat : Dusun II Desa Aman Damai Kec. Selesai Kab. Lingkat
   Dalam hal ini disebut Pihak Pertama (I)

Benar saya mempunyai sebidang Tanah Sawah yang terletak di Dusun VI Desa Aman Damai Kecamatan Sirapit Kabupaten Langkat dengan Luasnya ± 3.603 M² (Tiga Ribu Enam ratus Tiga Meter Persegi) ***Dengan No sertifikat Hak Milik 517 A.n SUDAR*** dengan batas-batas sebagai berikut :

Sebelah Utara	: berbatas dengan : Jl. Usaha tani	49,70	M
Sebelah Timur	: berbatas dengan : Parit Leningan	74	M
Sebelah Barat	: berbatas dengan : Parit Leningan	72,5	M
Sebelah Selatan	: berbatas dengan : Tanah Sudar	48,7	M

Selanjutnya pada hari ini Rabu Tanggal Lima Belas Bulan Mei Tahun Dua Ribu Dua Puluh Empat, Tanah Sawah tersebut diatas saya pihak pertama (I) Melepaskan Hak (Mengganti Rugikan) kepada Pihak Kedua (II).

2. Nama : SRI
   Umur : 38 Tahun
   Bangsa/Agama : Indonesia/Islam
   Pekerjaan : Karyawan Swasta
   Alamat : Jl. Bingai Kuala Langk.
   Dalam hal ini disebut Pihak Kedua (II)

Untuk Menguasai/Menguasahai Tanah Sawah tersebut di atas yang Luasnya ± 3.603 M² (Tiga Ribu Enam ratus Tiga Meter Persegi) dengan Uang Ganti Rugi Sebesar Rp.319.766.253,00, (Tiga Ratus Sembilan Belas Juta Tujuh Ratus Enam Puluh Enam Ribu Dua ratus Lima Puluh Tiga Rupiah) tanpa ada tuntutan dari saya maupun Pihak Ahli Waris lainya. Setelah saya dan Pihak Ahli Waris beserta Saksi-saksi lainya menanda Tangani surat ini. Maka Lepaslah /Gugurlah Hak dan Tanggung jawab saya dan Ahli Waris lainya terhadap Hak Tanah Sawah tersebut diatas. Untuk selanjutnya Tanah Sawah tersebut menjadi hak Milik Pihak Kedua (II).

Demikian surat Penyerahan Tanah Sawah ini di buat dengan sebenarnya, dengan Pikiran sehat dan tidak ada Paksaan dari Pihak manapun. Dan Apabila ternyata tidak benar maka saya bersedia dituntut sesuai dengan hukum yang berlaku serta tidak melibatkan aparat Pemerintah dan dapat dipergunakan sebagaimana mestinya.

Aman Damai, 20 Mei 2022

Pihak Pertama (I) Pihak Kedua (II)

SUDAR **SRI**

SAKSI :
1. KADUS VI (SUDI HARIYANTO) ( )
2. RT DUSUN VI/SUWONDO ( )
3. RT DUSUN VI/ SUHENDRA ( )

Mengetahui:
KEPALA DESA AMAN DAMAI
KECAMATAN SIRAPIT

SAKSI KELUARGA :
1. BENI LEKSMANA ( )
2. DICKI FIRMANSYAH ( )
3. SURIANTO ( )

SUGIMAN

SKETSA TANAH SAWAH

ATAS NAMA : SRI
LUAS TANAH : ± 3.603 M²
LOKASI : DUSUN VI DESA AMAN DAMAI KECAMATAN SIRAPIT

UTARA

UTARA
JL. USAHA TANI
49,70 M

BARAT
PARIT LENINGAN
72,5 M

TIMUR
PARIT LENINGAN
74 M

SELATAN
TANAH SUDAR
48,7 M

NB: Denah Tanah ini Sesuai Dengan Aslinya

SAKSI PENGUKUR:
1. KADUS VI (SUDI HARIYANTO) ( )
2. RT DUSUN VI/SUWONDO ( )
3. KADUS III/HERDIANTO ( )
4. HERMAN SITEPU ( )
5. SURIANTO ( )

Mengetahui;
KEPALA DESA AMAN DAMAI
KECAMATAN SIRAPIT

SAKSI PERINGGAN:
1. SUDAR ( )

(SUGIMAN)

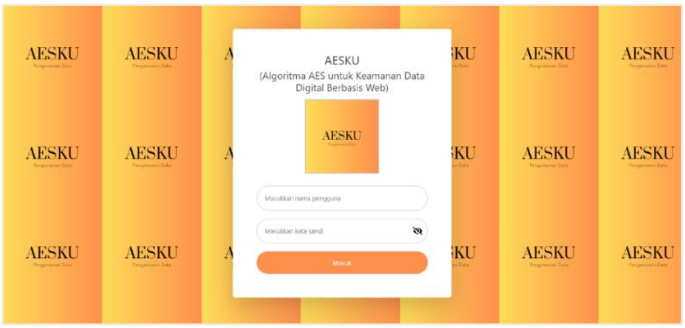
Gambar 2. Sampel Data Digital

4. Hasil Penelitian

Hasil Eksekusi Aplikasi Web

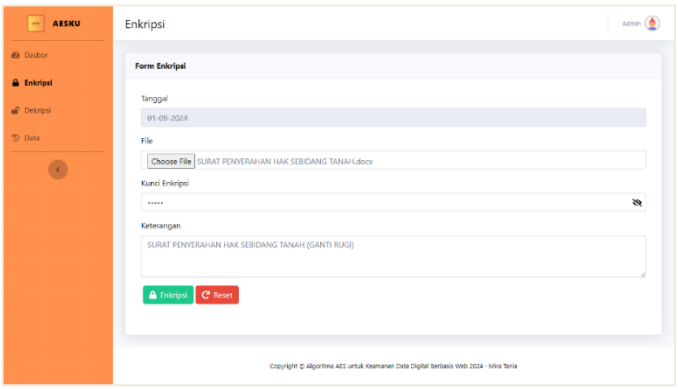
Pada tahap ini, penulis akan membahas mengenai hasil dari implementasi algoritma AES 128 bit. Hasil dari aplikasi ini adalah file data digital surat penyerahan hak sebidang tanah di Kantor Desa Aman Damai yang telah dienkripsi dan didekripsi. Berikut adalah tampilan atau interface dari program yang telah dibuat.

1. Halaman *Login*
   Halaman *login* pada aplikasi *web* ini dibuat untuk memastikan keamanan akses pengguna ke halaman utama. Pengguna harus memasukkan nama pengguna dan kata sandi yang valid untuk dapat masuk ke dalam aplikasi. Setelah data yang dimasukkan diverifikasi dan cocok dengan informasi yang terdaftar, pengguna akan diarahkan ke halaman utama aplikasi. Namun, jika nama pengguna atau kata sandi yang dimasukkan salah, akses akan ditolak dan pengguna tidak akan bisa masuk. Tampilan halaman *login* dapat dilihat pada gambar berikut.



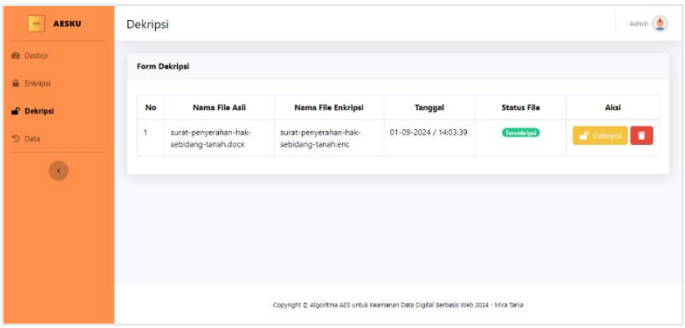
Gambar 3. Tampilan Halaman Login

2. Halaman Enkripsi
   Halaman enkripsi adalah halaman yang digunakan untuk melakukan proses enkripsi terhadap *file* data digital yang diunggah oleh pengguna. Halaman ini menjadi titik fokus dari penerapan enkripsi AES 128 bit. Terdapat *form* untuk mengunggah *file* yang akan dienkripsi. Tampilan halaman enkripsi dapat dilihat pada gambar berikut.



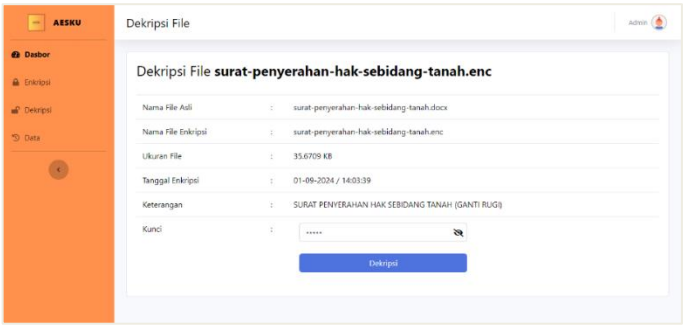
Gambar 2. Tampilan Halaman Enkripsi

3. Halaman Dekripsi Utama/Daftar *File* Terenkripsi
   Halaman dekripsi utama/daftar *file* terenkripsi merupakan halaman di mana *file* data digital yang telah dienkripsi dapat didekripsi kembali. Halaman ini menampilkan *file* yang telah dienkripsi di mana pengguna juga dapat menghapus *file* yang ada. Ketika pengguna mengklik tombol "Dekripsi", maka pengguna akan dialihkan ke halaman berikutnya, yaitu halaman dekripsi *file*. Tampilan halaman dekripsi utama/daftar *file* terenkripsi dapat dilihat pada gambar berikut.



Gambar 5. Tampilan Halaman Dekripsi Utama/Daftar File Terenkripsi

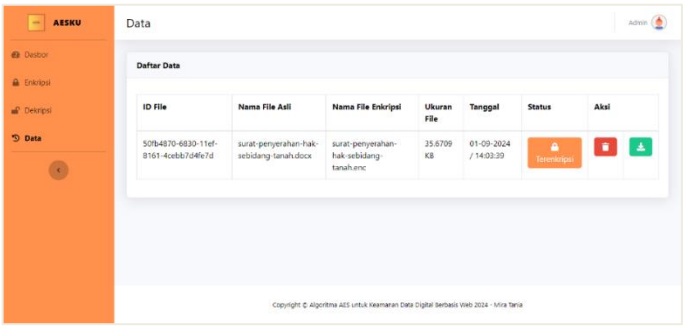
4. Halaman Dekripsi *File*
   Halaman dekripsi *file* adalah halaman di mana pengguna dapat mendekripsi *file* data digital yang telah dienkripsi sebelumnya. Untuk melakukan dekripsi, pengguna harus memasukkan kunci yang sama yang digunakan saat proses enkripsi awal. Tampilan halaman dekripsi *file* dapat dilihat pada gambar berikut.



Gambar 3. Tampilan Halaman Dekripsi File

5. Halaman Data

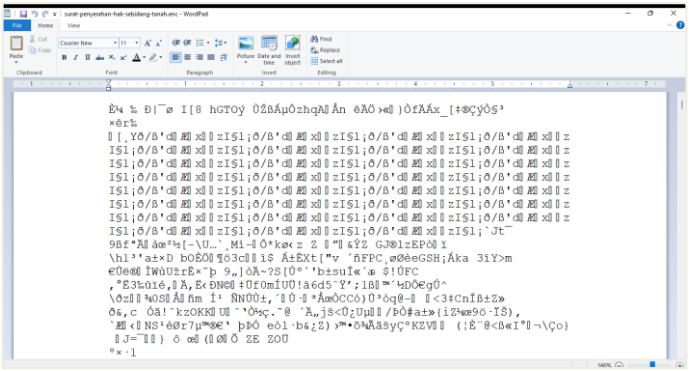
Halaman data menampilkan daftar data yang telah dienkripsi atau didekripsi oleh pengguna. Pada halaman ini, pengguna dapat melihat status data, apakah sudah terenkripsi atau terdekripsi. Pengguna juga memiliki opsi untuk menghapus dan mengunduh data tersebut. Tampilan halaman data dapat dilihat pada gambar berikut.



Gambar 4. Tampilan Halaman Data

6. Hasil Enkripsi

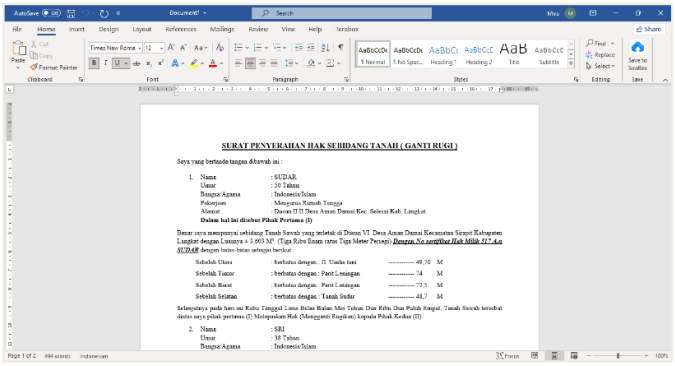
Hasil enkripsi dengan menggunakan algoritma AES 128 bit menghasilkan *file* dengan ekstensi *.enc. *File* ini dapat dibuka menggunakan aplikasi edit teks seperti *wordpad.* Hasil enkripsi dari penelitian ini adalah *file* yang berisi *ciphertext* data digital surat penyerahan hak sebidang tanah di Kantor Desa Aman Damai. Hasil enkripsi dapat dilihat pada gambar berikut.



Gambar 5. Hasil Enkripsi

7. Hasil Dekripsi

Hasil dari dekripsi menggunakan algoritma AES 128 bit menghasilkan *file* dengan ekstensi yang sama seperti bentuk awalnya. Misalnya, jika *file* yang dienkripsi berbentuk *word*, maka hasil dekripsinya juga akan berbentuk *file word*. Berikut ini adalah hasil dekripsi dari *file* data digital surat penyerahan hak sebidang tanah di Kantor Desa Aman Damai. Hasil dekripsi dapat dilihat pada gambar berikut.



Gambar 6. Hasil Dekripsi

Pembahasan

Dalam tahap ini, penulis akan menjelaskan tentang implementasi AES 128 bit pada *file* data digital surat penyerahan hak sebidang tanah di Kantor Desa Aman Damai.

a. Input *file* data digital
   Tahap pertama dalam mengoperasikan aplikasi adalah mengunggah *file* data digital ke dalam *form* enkripsi. *File* yang diunggah harus memiliki salah satu ekstensi berikut: doc, docx, txt, pdf, xls, dan xlsx dengan ukuran maksimal 6 MB. Jika ekstensi dan ukuran *file* tidak memenuhi kriteria ini, aplikasi tidak akan dapat melakukan proses enkripsi.
b. Input kunci simetri
   Tahap berikutnya adalah memasukkan kunci simetri untuk memulai proses enkripsi. Kunci simetri ini berfungsi untuk dekripsi atau pemulihan *file* yang telah dienkripsi ke bentuk aslinya. Kunci simetri harus memiliki maksimal 16 karakter, sesuai dengan algoritma enkripsi yang digunakan, yaitu AES 128 bit.
c. Proses enkripsi
   Tahap berikutnya adalah proses enkripsi, yang terdiri dari beberapa tahapan utama, yaitu *AddRoundKey*, *SubBytes*, *ShiftRows*, dan *MixColumns*, dilakukan selama 9 putaran, dan *AddRoundKey*, *SubBytes*, serta *ShiftRows* untuk putaran terakhir.
d. Proses dekripsi
   Tahap akhir adalah proses dekripsi. *File* yang telah melalui tahap enkripsi dapat dilanjutkan ke tahap dekripsi untuk mengembalikan *file* ke bentuk aslinya dengan memasukkan kunci simetri.

5. Kesimpulan

Berdasarkan hasil dari penerapan aplikasi berbasis web dengan algoritma AES 128 bit pada file data digital surat penyerahan hak sebidang tanah di Kantor Desa Aman Damai, dapat disimpulkan bahwa: Aplikasi tersebut dapat digunakan untuk mengamankan file dengan format doc, docx, txt, pdf, xls, dan xlsx. Proses enkripsi dan dekripsi memerlukan waktu yang bervariasi tergantung pada ukuran file. File data sampel surat penyerahan hak sebidang tanah yang berukuran 36 KB memerlukan waktu sekitar 3 detik untuk diproses. Sementara itu, file dengan ukuran maksimal yaitu 6 MB memerlukan waktu sekitar 3 menit untuk diproses. Ukuran file asli tetap sama setelah proses enkripsi dan dekripsi, yang menunjukkan bahwa enkripsi dan dekripsi tidak mengubah ukuran file.

6. Daftar Pustaka

[1] S. Taylor, “Data Security,” CFI Education Inc. [Daring]. Tersedia pada: https://corporatefinanceinstitute.com/resources/data-science/data-security/
[2] S. M. T. Situmeang, “Penyalahgunaan Data Pribadi Sebagai Bentuk Kejahatan Sempurna Dalam Perspektif Hukum Siber,” *Sasi*, vol. 27, no. 1, hal. 38, 2021, doi: 10.47268/sasi.v27i1.394.
[3] M. Sihombing, J. N. Sitompul, dan T. A. Putri, “Implementasi Metode Kriptografi Advanced Encryption Standard (AES) untuk Proteksi Pesan Audio,” *MEANS (Media Inf. Anal. dan Sist.*, vol. 4, no. 1, hal. 37–45, 2019, doi: 10.54367/means.v4i1.317.
[4] K. B. Ziliwu, A. Maslan, dan H. Kremer, “Implementasi Caesar Cipher pada Algoritma Kriptografi dalam Penyandian Pesan Whatsapp,” *J. Comasie*, vol. 7, no. 2, hal. 117–125, 2022.
[5] M. Firman Aditya, W. Arfanda, dan V. Ndika purnama, “Studi Algoritma Kriptografi Kunci Simetris Pada Keamanan Data Dengan Metode Komparasi,” *J. Siteba*, vol. 2, no. 1, hal. 7–14, 2023, [Daring]. Tersedia pada: https://journal.iteba.ac.id/index.php/jurnalsiteba/index
[6] M. R. Andriyanto dan P. Sukmasetya, “Penerapan Algoritma Advanced Encryption Standard (AES) Untuk Keamanan Data Transaksi Pada Sistem E-Marketplace,” *J. Comput. Syst. Informatics*, vol. 4, no. 1, hal. 179–187, 2022, doi: 10.47065/josyc.v4i1.2451.