Analisis Algoritma Enkripsi AES Untuk Pengamanan Data Dalam Media Komunikasi Digital

Cantika Risky Ramadhana Pawestri[1*], Otto Santoso Putro[2], Vivi Apriya Mardani[3]

[1] *S1 Teknik Informatika*
Jl. Bhayangkara No 55, Tipes, Kec. Serengan, Kota Surakarta
[1]220103008@mhs.udb.ac.id

[2] *S1 Teknik Informatika*
Jl. Bhayangkara No 55, Tipes, Kec. Serengan, Kota Surakarta
[2]220103026@mhs.udb.ac.id

[3] *S1 Teknik Informatika*
Jl. Bhayangkara No 55, Tipes, Kec. Serengan, Kota Surakarta
[3]220103040@mhs.udb.ac.id

Abstrak— **Permasalahan keamanan data dalam komunikasi digital, seperti email, pesan instan, dan media sosial, semakin penting di era digital saat ini karena informasi yang dikirimkan melalui media tersebut rentan terhadap akses ilegal, perubahan, atau penghapusan oleh pihak yang tidak berwenang. Penelitian ini bertujuan untuk menganalisis efektivitas algoritma enkripsi Advanced Encryption Standard (AES) dalam melindungi data digital. Metode yang digunakan adalah studi literatur mendalam yang melibatkan pengumpulan dan analisis data dari berbagai sumber terkait kriptografi, algoritma AES, dan model pemrogramannya, baik dari internet maupun buku. Selain itu, penelitian ini mencakup implementasi praktis AES untuk menguji keefektifannya dalam kondisi nyata menggunakan contoh plaintext "KULIAHDUTABANGSA" dan kunci "MOVINGTERUS". Hasil penelitian menunjukkan bahwa algoritma AES, melalui serangkaian transformasi yang kompleks namun efisien seperti SubBytes, ShiftRows, MixColumns, dan AddRoundKey, mampu memberikan keamanan yang kuat dan melindungi data dari upaya akses yang tidak sah. Implementasi praktis menunjukkan bahwa AES efektif dalam menghasilkan ciphertext yang aman, sehingga dapat direkomendasikan untuk digunakan oleh para praktisi dan organisasi dalam pengamanan data digital mereka. Penelitian lebih lanjut dianjurkan untuk menguji implementasi AES dalam berbagai kondisi dan dengan data yang lebih kompleks guna memastikan keandalannya dalam berbagai aplikasi praktis.**
Kata kunci— keamanan data, media komunikasi digital, enkripsi, Advanced Encryption Standard (AES), studi literatur, analisis teoretis.

Abstract— **Data security issues in digital communications, such as email, instant messaging, and social media, are increasingly important in the current digital era because information sent via these media is vulnerable to illegal access, change, or deletion by unauthorized parties. This research aims to analyze the effectiveness of the Advanced Encryption Standard (AES) encryption algorithm in protecting digital data. The method used is an in-depth literature study which involves collecting and analyzing data from various sources related to cryptography, the AES algorithm, and programming models, both from the internet and books. In addition, this research includes a practical implementation of AES to test its effectiveness in real conditions using the example of the plaintext "KULIAHDUTABANGSA" and the key "MOVINGTERUS". The research results show that the AES algorithm, through a series of complex but efficient transformations such as SubBytes, ShiftRows, MixColumns, and AddRoundKey, is able to provide strong security and protect data from unauthorized access attempts. Its practical implementation shows that AES is effective in producing secure ciphertext, so it can be recommended for use by practitioners and organizations in securing their digital data. Further research is recommended to test the implementation of AES under various conditions and with more complex data to ensure its efficiency in various practical applications.**
Keywords— data security, digital communication media, encryption, Advanced Encryption Standard (AES), literature study, theoretical analysis.

I. PENDAHULUAN

Kemajuan teknologi saat ini memungkinkan orang untuk berkomunikasi dan berbagi data serta informasi tanpa dibatasi oleh jarak atau waktu. Dengan meningkatnya kebutuhan akan keamanan informasi yang dipertukarkan, tuntutan terhadap ketersediaan data dan sistem keamanan informasi yang lebih baik untuk melindungi data dari ancaman pencurian data juga meningkat. Oleh karena itu, pengembangan metode pembelajaran ilmiah untuk melindungi data menjadi dampak positif dari adanya sistem keamanan yang melindungi data yang dikirimkan melalui jaringan komunikasi.[1]

Penggunaan teknologi informasi, media, dan komunikasi bisa mempengaruhi gaya hidup masyarakat seiring dengan kemajuan zaman. Hal ini menyebabkan meningkatnya penipuan melalui berbagai media komunikasi. Penipuan ini marak dilakukan oleh pihak-pihak yang tidak ingin bertanggung jawab untuk memperoleh keuntungan dari masyarakat yang kurang memahami hukum yang telah berlaku. [2]

Di sisi lain, penggunaan berbagai aplikasi media sosial berdampak pada keamanan data pengguna, membuat data pribadi rentan dieksploitasi oleh pihak yang tidak bertanggung jawab, seperti pelaku kejahatan siber. Data ini bisa disalahgunakan untuk penipuan, pencurian

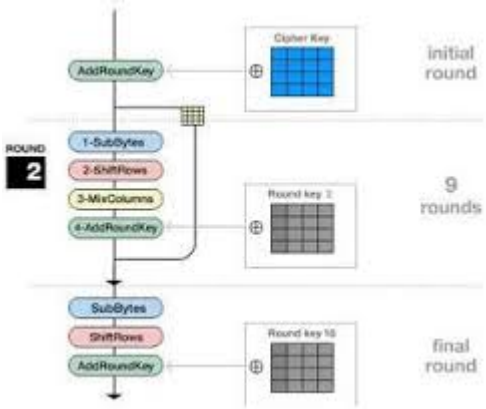
identitas, penyebaran identitas, serta pemerasan dan pelecehan online. Untuk mengatasi masalah keamanan data pada aplikasi media sosial, dibutuhkan sistem keamanan yang dapat mencegah hal-hal yang tidak diinginkan terhadap data pengguna.[3]

Teknologi informasi sangat penting dalam berbagai aspek kehidupan sehari-hari seperti pemerintahan, kesehatan, pendidikan, perbankan, pertanian, dan lembaga lainnya. Komputer digunakan untuk terhubung satu sama lain melalui jaringan dengan berbagai metode transmisi data.[4]

Penilaian terhadap nilai informasi dalam setiap konteks memungkinkan upaya pemindahan atau pencurian informasi oleh pihak yang tidak sah. Jenis media penyimpanan dan penyebaran data atau informasi menjadi faktor yang menjelaskan mengapa informasi dapat dengan mudah diakses oleh pihak yang tidak bertanggung jawab. Kriptografi adalah studi tentang teknik matematika untuk mengamankan pesan atau informasi asli (plaintext) sehingga menjadi tersembunyi (ciphertext), yang kemudian dapat dikembalikan ke bentuk aslinya. Kriptografi melibatkan tiga elemen kunci, enkripsi, dan dekripsi yang krusial dalam prosesnya.[5]

Dengan pemahaman yang lebih mendalam tentang AES, penelitian ini bertujuan untuk memberikan rekomendasi kepada para praktisi dan organisasi tentang penggunaan AES dalam pengamanan data digital mereka. Selain itu, penelitian ini juga mendorong penelitian lebih lanjut untuk menguji implementasi AES dalam berbagai kondisi dan dengan data yang lebih kompleks guna memastikan keandalannya dalam berbagai aplikasi praktis.

Pada algoritma enkripsi AES, dapat digambarkan seperti pada gambar dibawah ini.



Gambar 1. Algoritma Enkripsi AES

Dalam proses enkripsi, teks asli diubah menjadi suatu state. Sebelum ronde pertama, blok teks dicampur dengan kunci ronde ke-0 melalui transformasi yang disebut AddRoundKey. Setelah itu, dari ronde pertama hingga ronde ke-(Nr-1), dengan Nr sebagai jumlah total ronde, AES menggunakan empat jenis transformasi:

1) SubBytes, untuk substitusi. Yang biasanya menggunakan tabel S-Box untuk menjadi acuan

	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	01	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	04	c7	23	c3	18	96	05	9a	07	12	80	e2	eb	27	b2	75
4x	09	83	2c	1a	1b	6e	5a	a0	52	3b	d6	b3	29	e3	2f	84
5x	53	d1	00	ed	20	fc	b1	5b	6a	cb	be	39	4a	4c	58	cf
6x	d0	ef	aa	fb	43	4d	33	85	45	f9	02	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	06	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	08
cx	ba	78	25	2e	1c	a6	b4	c6	e8	dd	74	1f	4b	bd	8b	8a
dx	70	3e	b5	66	48	03	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

Gambar 2. Tabel S-Box

2) ShiftRows, untuk permutasi.
3) MixColumns, untuk pengacakan.
4) AddRoundKey, untuk penambahan kunci.

II. METODOLOGI PENELITIAN

Studi literature dilakukan dengan cara mengumpulkan data dan mempelajari segala macam informasi yang berhubungan dengan kriptografi, algoritma AES dan yang berhubungan dengan model pemogramannya, bisa melalui internet dan buku.

III. HASIL DAN PEMBAHASAN

A. Sejarah Kriptografi

Istilah "kriptografi" berasal dari bahasa Yunani, terdiri dari dua kata: "crypto" yang berarti rahasia dan "graphia" yang berarti tulisan. Kriptografi merupakan ilmu yang mempelajari teknik menyembunyikan pesan. Dalam penerapannya, kriptografi adalah metode enkripsi atau penyandian data yang hanya dapat dimengerti atau memiliki makna bagi sekelompok pengguna tertentu.[6]

Kriptografi adalah ilmu dan seni yang bertujuan melindungi kerahasiaan pesan dengan mengubahnya menjadi bentuk yang tidak dapat dimengerti. Dalam bidang ini, terdapat dua proses utama: enkripsi dan dekripsi. Pesan yang akan dienkripsi disebut plaintext (teks biasa) karena dapat dibaca dan dipahami oleh siapa saja. Algoritma yang digunakan untuk enkripsi dan dekripsi plaintext melibatkan penggunaan kunci tertentu. Pesan yang telah dienkripsi dikenal sebagai ciphertext atau teks sandi.[7]

Proses utama dalam kriptografi, seperti enkripsi dan dekripsi, bergantung pada kunci untuk mengamankan dan memulihkan informasi. Tanpa kunci, memulihkan data tersebut akan menjadi sangat sulit dan mungkin tidak berhasil sama sekali. Dalam kriptografi klasik, teknik enkripsi menggunakan metode simetris.[8] Untuk menjalankan proses kriptografi secara efisien, terdapat empat elemen utama yang saling terkait:

1. Plain Text: Ini adalah pesan asli yang dikirim selama proses komunikasi. Plain Text akan mengalami proses enkripsi dan dekripsi.
2. Cipher Text: Pesan yang tersandi setelah Plain Text dienkripsi menggunakan proses kriptografi. Cipher Text dapat dikembalikan ke bentuk aslinya (Plain Text) dengan menggunakan Key yang sesuai.
3. Cryptography Key: Kunci yang digunakan untuk melakukan enkripsi dan dekripsi dalam proses kriptografi. Tanpa kunci yang tepat, proses enkripsi dan dekripsi tidak akan berjalan efektif. Kunci ini merupakan informasi penting yang mengontrol proses kriptografi.
4. Encryption Decryption Algorithm: Komponen terakhir yang penting dalam proses kriptografi adalah algoritma yang digunakan untuk melakukan enkripsi dan dekripsi.[9]

B. Sejarah AES

Pada tahun 1997, US National Institute of Standards and Technology (NIST) memperkenalkan Advanced Encryption Standard (AES) untuk menggantikan Data Encryption Standard (DES). AES dikembangkan dengan tujuan meningkatkan keamanan di berbagai sektor. Algoritma AES dirancang dengan ukuran minimum blok input sebesar 128-bit dan mendukung tiga ukuran kunci: 128-bit, 192-bit, dan 256-bit.

Kriptografi adalah ilmu yang mempelajari cara melindungi informasi. Keamanan ini tercapai dengan mengenkripsi informasi menggunakan kunci tertentu. Informasi yang belum dienkripsi disebut plaintext, sementara setelah dienkripsi disebut ciphertext. Menjaga keamanan informasi sangat penting agar tidak disalahgunakan atau jatuh ke tangan yang tidak berwenang. Informasi tersebut bisa berupa kata sandi, nomor kartu kredit, atau data pribadi lainnya.

Upaya untuk menjaga kerahasiaan informasi sudah ada sejak lama. Kaisar Romawi Julius Caesar menggunakan metode enkripsi sederhana dengan menggeser setiap huruf dalam pesan dengan nilai tertentu. Meskipun metode ini sangat aman pada zamannya, sekarang mudah dipecahkan dengan kekuatan komputasi modern sehingga tidak lagi digunakan. Banyak algoritma kriptografi telah diciptakan oleh para kriptografer, dan berbagai upaya telah dilakukan oleh cracker untuk memecahkannya. Hal ini mendorong pengembangan algoritma yang lebih aman secara kriptografis. [10]

Perkembangan kriptografi yang paling signifikan terjadi pada tahun 1976 ketika Whitfield Diffie dan Martin Hellman menerbitkan tesis berjudul New Directions in Cryptography. Dalam tesis tersebut, mereka memperkenalkan konsep kunci publik yang revolusioner dan metode baru untuk pertukaran kunci yang keamanannya didasarkan pada logaritma diskrit. Walaupun mereka belum memiliki skema enkripsi kunci publik yang praktis pada saat itu, gagasan

ini memicu minat dan aktivitas besar dalam komunitas kriptografi.

Pada tahun 1978, Rivest, Shamir, dan Adleman menciptakan skema enkripsi kunci publik pertama yang dikenal sebagai RSA (Rivest, Shamir, and Adleman). RSA didasarkan pada masalah matematika kompleks yang melibatkan faktorisasi bilangan besar, yang mendorong upaya untuk menemukan metode faktorisasi yang lebih efisien. Selain RSA, skema kunci publik praktis lainnya ditemukan oleh ElGamal, yang juga berdasarkan masalah logaritma diskrit.

Salah satu kontribusi utama dari kriptografi kunci publik adalah tanda tangan digital. Pada tahun 1991, standar internasional pertama untuk tanda tangan digital berdasarkan skema kunci publik RSA diperkenalkan. Pada tahun 1994, pemerintah Amerika Serikat mengadopsi standar tanda tangan digital yang menggunakan skema kunci publik ElGamal.

Pencarian skema kunci publik baru dan pengembangan mekanisme kriptografi yang ada serta pembuktian keamanannya terus berlangsung dengan cepat. Standar dan infrastruktur terkait kriptografi terus dibangun, dan produk-produk keamanan terus dikembangkan untuk memenuhi kebutuhan keamanan informasi di masyarakat.[11]

C. Implementasi algoritma AES

Pada bagian ini, penulis akan memberikan sebuah gambaran tentang bagaimana algoritma enkripsi AES bekerja saat penyandian (enkripsi). Disini sebagai contoh mengubah plainteks : KULIAHDUTABANGSA menjadi ciphertext menggunakan kata kunci : MOVINGTERUS. Berikut merupakan penyelesaiannya :

Langkah pertama masukkan semua huruf ke dalam tabel-tabel dibawah ini.

Plainteks

Tabel 1. Tabel Plainteks

K	U	L	I
A	H	D	U
T	A	B	A
N	G	S	A

Chiperkey

Tabel 2. Tabel Chiperkey

M	O	V	I
N	G	T	E
R	U	S	M
O	V	I	N

Langkah selanjutnya adalah konversi semua isi dalam tabel kedalam bentuk Heksadesimal

Plainteks

Tabel 3. Konversi Plainteks

4B	55	4C	49
41	48	44	55
54	41	42	41
42	41	4E	47

Chiperkey

Tabel 4. Konversi Chiperkey

4D	4F	56	49
4E	47	54	45
52	55	53	00
00	00	00	00

Jika sudah saatnya melakukan 4 tahap pada algoritma AES , diantaranya yaitu :

1. AddRoundKey. Dalam proses ini, state heksadesimal dari plaintext dan cipherkey digabungkan menggunakan operasi XOR, menghasilkan state 128 berikut.

Tabel 5. AddRoundKey

06	1A	1A	00
0F	0F	10	10
06	14	11	41
42	41	4E	47

2. SubBytes. Dalam proses ini, hasil dalam AddRoundKey diubah menggunakan tabel S-Box.

Tabel 6. SubBytes

6F	A2	A2	63
76	76	CA	CA
6F	FA	82	09
2C	83	2F	A0

3. ShiftRows. Proses ini adalah memindahkan isi dari SubBytes dari baris ke 2 s/d 4 dengan urutan 1,2,3 kearah kiri. Yang digambarkan sebagai berikut.

Tabel 7. ShiftRows

6F	A2	A2	63
76	CA	CA	76
82	09	6F	FA
A0	2C	83	2F

4. MixColumns
   Dalam proses ini menggunakan matriks sebagai berikut.

Tabel 8. Matriks

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

Kemudian pada blok yang berwarna biru dikalikan dengan kolom pertama pada hasil ShiftRows. Disini penulis menggunakan kalkulator biner untuk mempermudah perhitungan yang hasilnya sebagai berikut.

02 X 6F = 10 X 01101111
= 11011110
03 X 76 = 11 X 01110110
= 10011010
01 X 82 = 1 X 10000010
= 10000010
01 X A0 = 1 X 10100000
= 10100000

Hasil akhir
11011110
10011010
10000010
10100000

= 01100110 = 66 bilangan heksa pada baris 1 kolom 1

IV. KESIMPULAN

Penelitian ini menyoroti masalah utama terkait keamanan data dalam komunikasi digital seperti email, pesan instan, dan media sosial, yang memerlukan metode efektif untuk melindungi informasi dari akses ilegal, perubahan, atau penghapusan. Analisis menunjukkan bahwa algoritma Advanced Encryption Standard (AES) adalah salah satu metode enkripsi paling populer karena kecepatan, efisiensi, dan kemampuannya memberikan keamanan yang kuat, dengan bekerja melalui serangkaian transformasi berulang seperti SubBytes, ShiftRows, MixColumns, dan AddRoundKey untuk memastikan keamanan data. Implementasi AES pada contoh plaintext "KULIAHDUTABANGSA" dengan kunci "MOVINGTERUS" berhasil menghasilkan ciphertext yang aman, menunjukkan efektivitas algoritma ini dalam melindungi data digital. Disarankan agar para praktisi dan organisasi menggunakan AES untuk melindungi data digital mereka, mengingat kecepatan dan efisiensinya. Penelitian lebih lanjut juga disarankan untuk menguji implementasi AES dalam berbagai kondisi dan dengan data yang lebih kompleks guna memastikan keandalannya dalam berbagai aplikasi praktis.

REFERENSI

[1] M. Azhari, D. I. Mulyana, F. J. Perwitosari, and F. Ali, "Implementasi Pengamanan Data pada Dokumen Menggunakan Algoritma Kriptografi Advanced Encryption Standard (AES)," Jurnal Pendidikan Sains dan Komputer, vol. 2, no. 01, pp. 163–171, Mar. 2022, doi: 10.47709/jpsk.v2i01.1390.

[2] I. Asih, R. Simbolon, I. Gunawan, I. O. Kirana, R. Dewi, and S. Solikhun, "Penerapan Algoritma AES 128-Bit dalam Pengamanan Data Kependudukan pada Dinas Dukcapil Kota Pematangsiantar," Journal of Computer System and Informatics (JoSYC), vol. 1, no. 2, 2020.

[3] M. Fajar, A. B. Kambodji, and I. A. Musdar, "Implementasi Algoritma Advanced Encryption Standard untuk Pengamanan Data Pengguna Aplikasi Media Sosial VirCle," Jurnal Algoritma, vol. 20, no. 2, pp. 398–409, Oct. 2023, doi: 10.33364/algoritma/v.20-2.1466.

[4] L. Silalahi, A. Sindar, and S. Pelita Nusantara, "Penerapan Kriptografi Keamanan Data Administrasi Kependudukan Desa Pagar Jati Menggunakan SHA-1," Jurnal Nasional Komputasi dan Teknologi Informasi, vol. 3, no. 2, 2020.

[5] N. Wulan, S. Sundari, and R. Dewi, "Prosiding SNASTIKOM: Seminar Nasional Teknologi Informasi & Komunikasi Paper Optimasi Algoritma AES Dengan Implementasi Parallel Dalam Pengamanan Data Digital," 2022.

[6] B. E. Widodo and A. S. Purnomo, "IMPLEMENTASI ADVANCED ENCRYPTION STANDARD PADA ENKRIPSI DAN DEKRIPSI DOKUMEN RAHASIA DITINTELKAM POLDA DIY," Jurnal Teknik Informatika (Jutif), vol. 1, no. 2, pp. 69–77, Dec. 2020, doi: 10.20884/1.jutif.2020.1.2.21.

[7] A. Eka Putri, A. Kartikadewi, and 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," Applied Information System and

Management (AISM), vol. 3, no. 2, pp. 69–78, Jan. 2021, doi: 10.15408/aism.v3i2.14722.

[8] C. Umam and D. Fadillah, "Kombinasi Steganografi LSB dan Kriptografi AES dalam Sekuriti Teks Rahasia Pada Citra Berwarna," 2 st Proceeding STEKOM, vol. 2022, 2022.

[9] D. Hulu, B. Nadeak, and S. Aripin, "Implementasi Algoritma AES (Advanced Encryption Standard) Untuk Keamanan File Hasil Radiologi di RSU Imelda Medan," vol. 4, no. 1, 2020, doi: 10.30865/komik.v4i1.2590.

[10] S. Oktaviani, F. Rizky, and I. Gunawan, "Analisis Keamanan Data Dengan Menggunakan Kriptografi Modern Algoritma Advance Encryption Standar (AES)," Jurnal Media Informatika, vol. 4, no. 2, pp. 97–101, Jun. 2023, doi: 10.55338/jumin.v4i2.435.

[11] "BAB II TEORI PENUNJANG 2.1 Kriptografi 2.1.1 Sejarah Kriptografi," 2024. Accessed: Jun. 15, 2024. [Online]. Available: http://eprints.umg.ac.id/4342/3/15.%20BAB%20II.pdf