ADIJAYA
Jurnal Multidisiplin
https://e-journal.naureendigition.com/index.php/mj
Vol. 01. No. 02, 2023, Hal. 380–387
E-ISSN : 2964-7606

ANALISIS PROSES ENKRIPSI ALGORITMA KRIPTOGRAFI MODERN *ADVANCED ENCRYPTION STANDARD* (AES)

Umami Wahyuningsih[1], Muhlis Tahir[2], Adinda Dwi Putri Andreani[3], Alfian Firdausi[4], Anggi Indri Wijayaningrum[5], Moch. Nasihuddin[6], Rikanawati[7], Aliffia Nurrohmah Zulkarnain[8]
wahyu.umami24@gmail.com muhlis.tahir@trunojoyo.ac.id
andreaniadinda05@gmail.com aliffianz022001@gmail.com
indrianggi98@gmail.com mohammadnasih331@gmail.com
rikanawati1704@gmail.com alfiancalonpresiden@gmail.com
Fakultas Ilmu Pendidikan, Universitas Trunojoyo Madura, Bangkalan

Abstrak Keamanan data adalah hal sangat perlu untuk diperhatikan, oleh karena itu penting adanya tindakan dalam mengamankan terhadap data yang dimiliki. Enkripsi dalam dunia kriptografi menjadi solusi untuk mengamankan data. Enkripsi yaitu suatu cara mengubah pesan menjadi pesan rahasia yang menampilkan kode-kode sehingga sulit dibaca. Dalam mengamankan data dikenal teknik kriptografi, salah satunya adalah *Advanced Encryption Standard (AES).* Setiap putaran dalam AES memerlukan hasil *key generation* dan melalui proses 4 variasi dasar yaitu *subbytes*, *shiftrows*, *mixcolumns*, dan *addroundkey*. Hasil dari penelitian ini adalah analisis algoritma keamanan data AES yang menghasilkan hasil enkripsi 128 bit.

Kata Kunci: *Advanced Encryption Standard,* Enkripsi, Keamanan Data, Kriptografi

Abstract *Data security is something that really needs to be considered, therefore it is important to take action to secure the data you have. Encryption in the world of cryptography is a solution for securing data. Encryption is a way of turning messages into secret messages that display codes that are difficult to read. In securing data, known cryptographic techniques, one of which is the Advanced Encryption Standard (AES). Each round in AES requires key generation results and goes through a process of 4 basic variations, namely subbytes, shiftrows, mixcolumns, and addroundkey. The results of this study are the analysis of the AES data security algorithm which produces 128-bit encryption results.*

Keywords: *Advanced Encryption Standard, Encryption, Data Security, Cryptography*

Pendahuluan

Perkembangan teknologi informasi di dunia sangat pesat, sehingga tidak dapat dipungkiri kebutuhan untuk melindungi data dari pihak yang tidak berwenang sangat penting. Hal itulah yang melahirkan ide untuk mengamankan data dan informasi khususnya untuk keamanan data. Secara tradisional, data dapat diamankan dengan banyak cara, misalnya saat mengirim pesan singkat, pesan tersebut ditulis di kertas panjang yang digulung di atas pohon (*scytale*), dan saat gulungan kertas dibuka, pesan tersebut berupa huruf yang sulit dan harus di enkripsi (Harahap, 2016). Kemudian Julius Caesar (Kaisar Romawi) mengamankan pesan dengan metode enkripsi sederhana, yakni dengan memindahkan karakter-karakter pesan dengan nilai tertentu. Cara ini sudah cukup aman pada masa itu.

Semakin pesatnya perkembangan zaman, ilmu keamanan data pun turut berkembang. Pada zaman ini, dikenal istilah kriptografi. Kriptografi adalah disiplin ilmu yang mempelajari cara agar informasi yang dikirimkan dapat tiba dengan keamanan terjamin pada penerimanya (Hayaty, 2020). Kriptografi juga semakin berkembang, dimana mula-mula hanya digunakan secara tradisional, saat ini telah dikembangkan menggunakan bantuan perhitungan matematis dan teori bilangan dalam proses pembuatan kunci, enkripsi dan deskripsi serta pengolahan data komputer.

Dalam buku David Kahn, sejarah kriptografi ditulis secara lengkap yaitu sebagai *The Coderbreakers* pada tahun 1963. Setelah 4000 tahun, David Khan menceritakan sejak bangsa Mesir, pada saat itu Mesir masih berupa hieroglif yang non-baku untuk menulis pesan di piramida. Selama 400 tahun, orang Yunani menggunakan alat yang disebut *scytale* untuk menyampaikan pesan. *Scytale* adalah secarik kertas panjang yang dililitkan pada sebatang kayu, artinya pesan ditulis mendatar, baris demi baris. Saat kertas dilepas, pesan menjadi sandi yang sulit dibaca. Begitulah orang Yunani mengirimkan pesan rahasia kepada mereka yang terlibat. Kriptografi mulai diteliti dan mulai digunakan untuk keamanan informasi pada abad ke-20, dan sering kita lihat di arena militer.

Gambar 1. *Scytale*
Sumber: (Harahap, 2016)

Kriptografi (*cryptography*) berasal dari bahasa Yunani yang terdiri dari dua suku kata, yaitu *crypto* dan *graphia*. *Crypto* berarti "bersembunyi", sedangkan *graphia* bearrti "menulis". Kriptografi adalah ilmu dan seni untuk melindungi pesan (Hulu, *et al.*, 2020). Kata "seni" dalam pengertian diatas berarti cara yang unik untuk menjaga pesan. Kriptografi mempelajari teknik matematik yang berkaitan dengan keamanan informasi (Hasugian, 2017). Sistem kriptografi adalah fitur yang memungkinkan untuk mengubah pesan yang jelas (*plaintext*) diubah menjadi pesan yang tersandi (*ciphertext*) (Tulloh et al., 2016). Proses tersebut dinamakan enkripsi dan sebaliknya, jika ingin menerjemahkan *chipertext* menjadi *plaintext* disebut deskripsi.

Dalam (Amrulloh & Ujianto, 2019), terdapat beberapa istilah dalam kriptografi seperti berikut :

a. *Plaintext*, merupakan pesan atau data yang dapat dibaca dan dipahami, berfungsi sebagai input untuk proses enkripsi dan output untuk proses deskripsi.
b. *Ciphertext*, adalah pesan atau data yang sulit dibaca dan menjadi inputan untuk proses deskripsi dan output untuk proses enkripsi.
c. Algoritma enkripsi, adalah rangkaian proses yang dilakukan pada *plaintext* dengan menggunakan kunci rahasia untuk menghasilkan *ciphertext.*

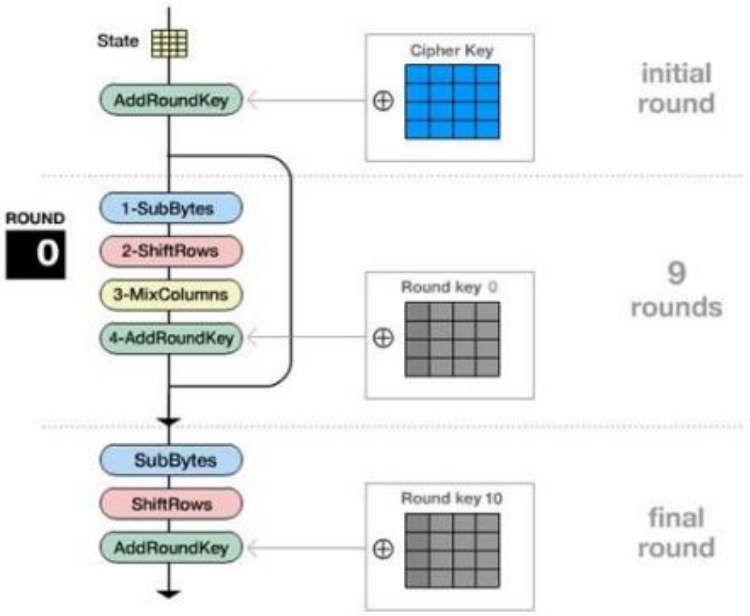
d. Algoritma deskripsi, adalah rangkaian proses yang mengeksekusi *ciphertext* menggunakan kunci rahasia untuk menghasilkan teks asli atau *plaintext*.
e. Kunci rahasia, adalah nilai yang digunakan untuk mengubah *plaintext* menjadi *ciphertext*.

Tujuan kriptografi adalah untuk melindungi kerahasiaan informasi yang terkandung dalam data sehingga tidak diungkapkan kepada orang yang tidak berwenang (Jamaludin et al., 2022). Tujuan utama dari kriptografi terdapat dalam empat aspek keamanan suatu sistem informasi, yaitu :

1. Kerahasiaan (*confidentially*), yakni layanan yang dirancang untuk menjaga pembacaan oleh orang yang tidak berwenang.
2. Otentikasi adalah layanan terkait identifikasi yang mengidentifikasi kebenaran pengirim dan penerima serta integritas sumber informasi.
3. Integritas data adalah layanan yang memastikan bahwa pesan adalah asli atau belum dirusak dalam pengiriman.
4. Non-repudation merupakan layanan yang mencegah mitra komunikasi untuk membantah, yaitu pengirim pesan menolak mengirim atau penerima pesan membantah menerima pesan.

Terdapat 2 jenis algoritma kriptografi berdasarkan kuncinya, yakni algoritma kriprografi kunci simetris dan algoritma kriptografi kunci asimetris (Arrijal, Efendi, & Susilo, 2016). Algoritma kunci simetris (algoritma enkripsi tradisional) yaitu algoritma yang kuncinya sama untuk proses enkripsi dan deskripsi. Sedangkan algoritma kunci asimetris yaitu algoritma dengan kunci yang berbeda di proses enkripsi dan deskripsi.

Salah satu jenis kriptografi modern adalah *Advanced Encryption Standard (AES).* Pada tahun 1997, National Institute of Standard and Technology (NIST) of United States merilis *Advanced Encryption Standard (AES)* sebagai pembaruan dari *Data Encryption Standard (DES)* (Murdowo, 2014). Algoritma AES berfungsi melindungi data dengan cara mengenkripsi dan mendeskripsi informasi dengan blok *ciphertext.* Proses enkripsi dalam AES terdiri dari 4 jenis variasi dasar, yaitu *SubBytes, ShiftRows, MixColumns,* dan *AddRoundKey*. Algoritma AES digunakan untuk mengenkripsi dan mendeskripsi data dengan panjang kunci yang berbeda yaitu 128 *byte*, 192 *byte* dan 256 *byte* (Handoyo & Subakti, 2020). Pada proses enkripsi, algoritma AES dapat digambarkan sebagai berikut.



Gambar 2. Algoritma Enkripsi AES
Sumber: (Prameshwari & Sastra, 2018)

Terdapat 5 tahap dalam proses enkripsi pada AES (Sihombing, *et al.*, 2019). Berikut tata cara enkripsi yang digunakan dalam algoritma AES, yaitu :

1. AddRoundKey : Proses ini pada awal putaran dengan meng-XOR-kan setuap *byte* dalam *state matrix* (*plaintext)* dengan setiap *byte* kunci enkripsi (*cipherkey*). Langkah ini sering juga disebut *initial round.*
2. SubBytes : Proses konversi *byte* dari state matriks hasil addroundkey menggunakan array pengganti (S-Box).

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

Gambar 2. Tabel S-Box
Sumber: (Erlangga, *et al.*, 2014)

3. Shiftrows : Proses pergeseran bit dimana bit paling kiri digeser ke bit paling kanan. Jumlah pergeseran setiap baris berbeda. Baris pertama tidak digeser, baris kedua digeser ke kiri satu *byte*, baris ketiga digeser ke kiri dua *byte*, dan seterusnya.
4. MixColumns : Proses perkalian matriks pada tiap kolom. Setiap kolom dalam matriks dikalikan dengan matris berikut :

$$\begin{bmatrix} 02 & 03 & 01 & 01 \\ 01 & 02 & 03 & 01 \\ 01 & 01 & 02 & 03 \\ 03 & 01 & 01 & 02 \end{bmatrix}$$

5. AddRoundKey : Proses operasi XOR setiap *byte* keluaran dari MixColumns dengan *roundkey.*

Oleh karena itu, penulis tertarik untuk menganalisis proses enkripsi pada algoritma *Advanced Encryption Standard* karena memiliki algoritma yang cukup sulit dalam mengamankan data.

Metode

Metode yang dipakai adalah perhitungan menggunakan algoritma *Advanced Encryption Standard* (AES) yang terdiri dari 4 variasi perhitungan dasar.

Hasil dan Pembahasan

Pada bagian pembahasan, Penulis memberikan gambaran tentang bagaimana algoritma AES bekerja saat melakukan penyandian (encrypting) pesan asli menjadi pesan rahasia. Disini akan mengubah teks plainteks menjadi ciphertext yaitu : INFORMATIKA HEBAT, yang akan diproses dengan kata kunci : KRIPTOGRAFI. Berikut merupakan gambaran dalam menyelesaikan perhitungan algoritma AES :

Masukkan Ke Kolom 4 x 4

Plainteks

I	N	F	O
R	M	A	T
I	K	A	H
E	B	A	T

Cipherkey

K	R	I	P
T	O	G	R
A	F	I	K
R	I	P	T

Konversi ke Heksadesimal

Plainteks

49	4E	46	4F
52	4D	41	54
49	4B	41	48
45	42	41	54

Cipherkey

4B	52	49	50
54	4F	47	52
41	46	49	4B
52	49	50	54

Initial Round

Didalam tahap initial round terdapat 4 tahap, diantaranya yaitu :

AddRoundKey

Pada proses ini state heksadesimal dari plaintext dan state heksadesimal dari cipherkey di-XOR-kan sehingga menghasilkan state 128 berikut ini.

02	1C	0F	1F
06	02	06	06
08	0D	08	03
17	0B	11	00

Proses SubBytes

Proses ini mengubah state hasil AddRoundKey menggunakan tabel S-Box.

02	1C	0F	1F
06	02	06	06
08	0D	08	03
17	0B	11	00

77	9C	76	C0
6F	77	6F	6F
30	D7	30	7B
F0	2B	82	63

Proses ShiftRows

77	9C	76	C0
6F	77	6F	6F
30	D7	30	7B
F0	2B	82	63

77	9C	76	C0
6F	77	6F	6F
30	D7	30	7B
F0	2B	82	63

77	9C	76	C0
6F	77	6F	6F
30	D7	30	7B
F0	2B	82	63

77	9C	76	C0
6F	77	6F	6F
30	D7	30	7B
F0	2B	82	63

77	**9C**	**76**	**C0**
6F	**77**	**6F**	**6F**
30	**D7**	**30**	**7B**
F0	**2B**	**82**	**63**

77	**9C**	**76**	**C0**
6F	**77**	**6F**	**6F**
30	**D7**	**30**	**7B**
63	**F0**	**2B**	**82**

Proses MixColumns

02	**03**	**01**	**01**
01	**02**	**03**	**01**
01	**01**	**02**	**03**
03	**01**	**01**	**02**

77
77
30
63

Cara penyelesaian :

02 X 77 = 10 X 01110111
= X ($X^6 + X^5 + X^4 + X^2 + X + 1$)
= $X^7 + X^6 + X^5 + X^3 + X^2 + X$
= 11101110

03 X 77 =11 X 01110111
= (X+1) ($X^6 + X^5 + X^4 + X^2 + X + 1$)
= ($X^7 + X^6 + X^5 + X^3 + X^2 + X$) ($X^6 + X^5 + X^4 + X^2 + X + 1$)
= $X^7 + X^4 + X^3 + 1$
= 10011001

01 X 30 = 1 X 00110000
= 00110000

01 X 63 = 1 X 01100011
= 01100011

Hasil Akhir Perhitungan

11101110
10011001
00110000
<u>01100011</u>
= 00100100 = 24 (bilangan heksa) untuk baris 1 kolom 1

Cara pengerjaan untuk baris dan kolom selanjutnya tetap sama hingga menghasilkan nilai dari Round 1 yaitu :

24	CA	0D	34
F1	3F	FB	11
21	0E	6E	63
F5	20	93	50

Selanjutnya masuk ke proses AddRoundKey, dalam proses ini hasil state 128 bit akan di-XOR-kan dengan round key, yaitu kunci hasil dari proses pembangkitan kunci. Di awal enkripsi state plaintext akan di-XOR-kan dengan cipherkey. Kemudian plaintext yang sudah di XOR kan dengan cipherkey akan melalui 4 proses yakni *SubBytes, ShiftRows, MixColumns* dan *AddRoundKey.* Setelah itu hasilnya akan di-XOR-kan dengan roundkey hasil expandkey yang pertama. Setelah ditemukan hasilnya, itu merupakan hasil state pada round 1. State tersebut akan melalui proses perputaran round lagi hingga putaran ke-10. Di putaran ke-10 tidak perlu di *MixColumns*-kan. Setelah itu baru didapat hasil *ciphertext* dari *plaintext* yang sudah dimasukkan.

Kesimpulan

Algoritma AES adalah algoritma yang istimewa di mana setiap putaran memiliki proses detailnya tersendiri sehingga dapat menciptakan keamanan data yang baik. Sebagaimana tujuan dari kriptografi sendiri yakni mengamankan data dari orang yang tidak berwenang. Proses enkripsi dengan algoritma ini menjadikan pesan lebih terjaga keamanannya. Adapun proses yang dilalui oleh algoritma AES adalah pertama *plaintext* dan *cipherkey* akan dikoversikan ke kode ASCII sebagai bilangan heksadesimal dan kemudian dibentuk menjadi state matriks 4x4. Kemudian akan mengalami proses round sebanyak 10 putaran dengan bantuan kunci hasil expand key di setiap round dengan melalui 4 variasi dasar yakni *SubBytes, ShiftRows, MixColumns,* dan *AddRoundKey.*

Daftar Referensi

Amrulloh, A., & Ujianto, E. I. H. (2019). Kriptografi Simetris Menggunakan Algoritma Vigenere Cipher. *Jurnal CoreIT*, *5*(2), 71–77.

Arrijal, I. M., Efendi, R., & Susilo, B. (2016). Penerapan Algoritma Kriptografi Kunci Simetris Dengan Modifikasi Vigenere Cipher Dalam Aplikasi Kriptografi Teks. *Pseudocode*, *3*(1), 69–82. https://doi.org/10.33369/pseudocode.3.1.69-82

Erlangga, A., Beeh, Y. R., & Wowor, A. D. (2014). *S-Box Dinamis Algoritma AES untuk Kriptografi File pada Android Mobile Phone*.

Handoyo, J., & Subakti, Y. M. (2020). Keamanan Dokumen Menggunakan Algoritma Advanced Encryption Standard (Aes). *Jurnal SITECH : Sistem Informasi Dan Teknologi*, *3*(2), 143–152. https://doi.org/10.24176/sitech.v3i2.5865

Harahap, M. K. (2016). Analisis Perbandingan Algoritma Kriptografi Klasik Vigenere Cipher Dan One Time Pad. *InfoTekJar (Jurnal Nasional Informatika Dan Teknologi Jaringan)*, *1*(1), 61–64. https://doi.org/10.30743/infotekjar.v1i1.43

Hasugian, B. S. (2017). Peranan Kriptografi Sebagai Keamanan Sistem Informasi Pada Usaha Kecil Dan Menengah. *Jurnal Warta Edisi*, *53*(9), 2.

Hayaty, N. (2020). *Buku Ajar: Sistem Keamanan*.

Hulu, D., Nadeak, B., & Aripin, S. (2020). Implementasi Algoritma AES (Advanced Encryption Standard) Untuk Keamanan File Hasil Radiologi di RSU Imelda Medan. *KOMIK (Konferensi ...*, *4*, 78–86. https://doi.org/10.30865/komik.v4i1.2590

Jamaludin, J., Sulaiman, O. K., Tandungan, S., Putra, L. M., Yuswardi, Y., Yulianti, N., … others. (2022). *Kriptografi: Teknik Keamanan Data*. Yayasan Kita Menulis. Retrieved from https://books.google.co.id/books?id=1W1tEAAAQBAJ

Murdowo, S. (2014). Mengenal Proses Perhitungan Enkripsi Menggunakan Algoritma Kriptografi Advance Encryption Standard (Aes) Rijdnael. *INFOKAM Nomor I / Th. X/ Maret / 14*, *10*, 32–40. Retrieved from http://jurnal.amikjtc.com/index.php/jurnal/article/view/55

Prameshwari, A., & Sastra, N. P. (2018). Implementasi Algoritma Advanced Encryption Standard (AES) 128 Untuk Enkripsi dan Dekripsi File Dokumen. *Eksplora Informatika*, *8*(1), 52. https://doi.org/10.30864/eksplora.v8i1.139

Rasidin, A., Nugroho, A.J. (2022). Analisa Penggunaan Teknik Advanced Encryption (AES) dalam Kriptografi. *Jurnal Dinamika Universitas Muhammadiyah Tangerang,* 21-29.

Sihombing, M., Sitompul, J. N., & Putri, T. A. (2019). Implementasi Metode Kriptografi Advanced Encryption Standard (AES) untuk Proteksi Pesan Audio. *MEANS (Media Informasi Analisa Dan Sistem)*, *4*(1), 37–45. https://doi.org/10.54367/means.v4i1.317

Tulloh, A. R., Permanasari, Y., Harahap, E., Matematika, P., Matematika, F., Ilmu, D., & Alam, P. (2016). Kriptografi Advanced Encryption Standard (AES) Untuk Penyandian File Dokumen. *Jurnal Matematika UNISBA*, *Vol 2*(1), 1–8.

Wiharto, Y., Mufti. (2022). Implementasi *Advanced Encryption Standard 128* Sebagai Pengamanan Basis Data Obat-obatan Apotek. *Jurnal Teknik Informatika dan Sistem Informasi, Vol 8*(2), 335-350.