Jurnal Kendali Teknik dan Sains
Vol. 1, No. 2 April 2023
e-ISSN: 2986-3228; p-ISSN: 2986-4429, Hal 103-115
DOI: https://doi.org/10.59581/jkts-widyakarya.v1i2.314

Analisa Penyandian File Dokumen Kriptografi Menggunakan *Advanced Encryption Standard* (AES)

Terisha Sheline Shazhaq [1], Muhlis Tahir [2], Khoirul Amin Abidin [3], Vivia Auria [4], Diana Iis Maulidia [5], Dwi Fatkhul Mu'in [6], Moh Khoiruddin [7]
[1,2,3,4,5,6,7] Universitas Trunojoyo Madura
Korespondensi penulis: 190631100070@student.trunojoyo.ac.id

Abstract. *(Cryptography Advanced Encryption Standard (AES) for File Document Encryption). Advanced Encryption Standard (AES) is a cryptographic algorithms as a standard symmetric key encryption algorithm that used in current time. AES 128 has 1 blok plaintext with 128 bit sized, where in the process of cryptographic algorithms, first the plaintext is converted into hexadecimal-sized 4 x 4 matrices called the state, where each element of state has 1 byte size. The process of encryption on AES is the transformation towards the state repeatedly in the 10th round. Each round of AES requires one key result of the key generation using 2 basic transformation, i.e. substitution and transformation. AES encryption using 4 transformation by the following sequence: subbytes, shiftrows, mixcolumns, and addroundkey. On the other hand, the process of decryption is using the inverse of all the basic transformation of AES algorithm, except addroundkey. Therefore, the sequence of transformation on the decription is invshiftrows, invsubbytes, invmixcolumns, and addroundkey. In the data text, the encryption process is initiated with convertion the data text into ASCII code in hexadecimal numbers that are molded into the matrix 4 x 4 bytes. Next, do some basic transformation such as subbytes, shiftrows, mixcolumns, and addroundkey. However, when performing the transformation, the processed data on every trasformation is in the form of binary data obtained from the hexadecimal matrix. AES 128 bit cryptography have room 2^{128} keys which is a tremendous value and is considered secure to use to avoid the brute force attack.*

Keywords: *AES, file Encryption, symmetric key algorithm.*

Abstrak. *Advanced Encryption Standard* (AES) adalah algoritma enkripsi yang saat ini merupakan algoritma enkripsi kunci simetris standar. Dalam algoritma enkripsi AES-128, *blok plaintext* 128-bit pertama-tama diubah menjadi matriks heksadesimal 4x4 yang disebut *state*. Setiap ruang adalah 1 *byte*. Proses enkripsi AES adalah konversi ke status yang diulang dalam 10 putaran. Setiap putaran AES membutuhkan kunci keluaran

Received Februari 23, 2023; Revised Maret 22, 2023; Accepted April 25, 2023
* Terisha Sheline Shazhaq, *190631100070@student.trunojoyo.ac.id*

untuk menghasilkan kunci menggunakan dua transformasi yaitu substitusi dan transformasi. Proses enkripsi AES menggunakan 4 transformasi dasar dengan transformasi *Subbytes*, *Shift Rows*, *Mixcolumns*, dan *Addroundkey*. Selama proses dekripsi, inversi dari semua transformasi algoritma AES dasar digunakan, kecuali urutan transformasi *addroundkey invshiftrows*, *invsubbytes*, *addroundkey* dan *invmixcolumns*. Proses enkripsi data teks diawali dengan mengubah teks menjadi kode ASCII dengan bilangan heksadesimal yang dibentuk menjadi matriks berukuran 4x4 *byte*. Selain itu, beberapa transformasi dasar dilakukan, seperti *Subbytes*, baris pengganti, kolom campuran, dan kunci tambahan. Namun pada saat dilakukan transformasi, data yang diproses pada setiap transformasi berupa data biner dari matriks heksadesimal. Kriptografi AES-128-bit memiliki ruang kunci 2^{128}, yang merupakan nilai yang sangat besar dan dianggap aman untuk digunakan, menghindari *brute force attack*.

Kata kunci: AES, Penyandian file, Algoritma kunci simetris.

LATAR BELAKANG

Perkembangan teknologi informasi dan komunikasi saat ini membuat masyarakat dapat berkomunikasi dan bertukar informasi tanpa terhalang jarak dan waktu. Seiring dengan meningkatnya tuntutan akan keamanan kerahasiaan data yang dipertukarkan, hal ini menimbulkan tuntutan akan tersedianya sistem keamanan informasi dan data yang lebih baik untuk melindungi data dari berbagai ancaman. Oleh karena itu, pengembangan departemen yang mempelajari metode keamanan informasi berdampak positif pada persyaratan kegunaan sistem keamanan informasi yang melindungi data yang ditransfer atau dikirim melalui jaringan komunikasi. Ilmu yang mempelajari metode keamanan informasi dikenal dengan kriptografi.

Kriptografi adalah ilmu yang mempelajari teknik matematika yang berkaitan dengan aspek keamanan data dan informasi seperti validitas data, integritas data, dan otentikasi data. Sistem enkripsi adalah suatu fungsi yang dapat digunakan untuk mengubah pesan yang jelas (*plaintext*) menjadi pesan yang disandikan (*ciphertext*). Proses konversi ini disebut enkripsi (enkripsi). Sebaliknya, terjemahan dari *ciphertext*

ke *plaintext* disebut dekripsi. Satu atau lebih kunci enkripsi digunakan dalam proses enkripsi dan dekripsi.

Dalam bidang kriptografi dikenal dua konsep yang sangat penting yaitu enkripsi dan deskripsi. Proses pengiriman pesan melalui proses enkripsi yang mengubah teks asli (teks belakang) menjadi teks sandi. Proses enkripsi mempersulit orang yang tidak berwenang untuk mendapatkan informasi. Perlindungan ini diperlukan untuk menghindari penyadapan atau peretasan file yang berisi informasi penting bagi pengguna dan untuk menjaga keamanan integritas tersebut. Oleh karena itu diperlukan suatu algoritma yang dapat melindungi file yaitu algoritma AES (*Advanced Standard Encryption*).

Berdasarkan latar belakang yang telah diuraikan, maka perumusan masalah dalam penelitian ini sebagai berikut: “Bagaimana proses penyandian dengan *Advanced Encryption Standard* (AES)?”. Selanjutnya, tujuan dalam penelitian ini ialah untuk memahami proses penyandian dengan *Advanced Encryption Standard* (AES). Selain itu juga untuk mengetahui penerapan Algoritma kriptografi AES pada file teks serta dapat merancang dan menggunakan program pengamanan data teks metode Kriptografi AES.

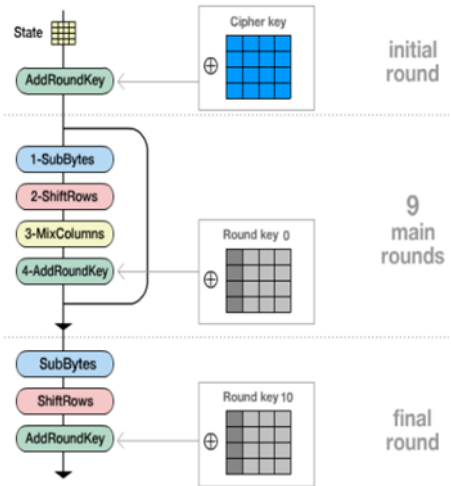
KAJIAN TEORITIS

AES adalah algoritma 2 simetris yang menggunakan kunci yang sama dalam proses enkripsi dan dekripsi. Algoritma AES memiliki tiga pilihan kunci, yaitu:AES 128-bit, AES 192-bit, dan AES 256-bit. Sebagai gambaran proses enkripsi pada algoritma Rijndael yang menggunakan blok 128bit dengan kunci 128bit adalah sebagai berikut:

a. *Initial Round* yaitu tahapan *AddRoundKey* yang melakukan XOR (*Exlusive OR*) antara state awal dari data masukan (*plaintext*) dengan *cipher key* (kunci *cipher*).

b. Putaran sebanyak *Nr* – 1 kali (*Round Nr-1*). Proses yang dilakukan pada setiap putaran adalah:
    1. *SubByte*: substitusi *byte* dengan menggunakan tabel substitusi (*S-Box*).
    2. *ShiftRow*: pergeseran baris-baris *array state* secara *wrapping*.
    3. *MixColumn*: mengacak data di masing-masing kolom *array state*.
    4. *AddRoundKey* yaitu melakukan XOR antara *state* sekarang dengan *round key*.
c. *Final round*: proses untuk putaran terakhir:
    1. *ByteSub*
    2. *ShiftRow*
    3. *AddRoundKey*.

Skema proses enkripsi pada AES dapat dilihat pada gambar 1 berikut:



Gambar 1. 1 Skema enkripsi AES

Berdasarkan analisis pada beberapa referensi dapat diketahui beberapa kelebihan dari AES (*Advanced Encryption Standard*) di antaranya:

a. Dengan jenis kunci simetris, kecepatan operasi (komputasi) lebih tinggi dibandingkan algoritma asimetris, sehingga dapat digunakan pada sistem *real-time* seperti GSM.
b. Panjang kunci AES setidaknya 128 bit, sehingga AES dapat menahan serangan pengambilan kunci yang luas dengan teknologi saat ini. Kunci 128-bit memiliki $2^{128} \approx 3{,}4 \times 10^{38}$ kemungkinan kunci. Jika kita menggunakan mesin dengan satu miliar prosesor paralel, yang masing-masing dapat menghitung kunci setiap pikodetik, akan diperlukan waktu 10^{10} tahun untuk mencoba semua kemungkinan kunci.

Kekuatan AES terletak pada sifat karakteristik bidang GF(28), di mana selalu ada bidang singular berhingga yang unik untuk setiap bilangan prima sehingga semua representasi GF(28) adalah isomorfik dan pemilihan polinomial biner dari derajat ke-8 m(x) tidak dapat direduksi, yaitu tidak dapat dibagi dengan angka apa pun di bidang kecuali 1 dan sebanding dengan bilangan prima di bidang itu sendiri.Pangkat ini didasarkan pada operasi matematika yang kompleks dan membutuhkan banyak sumber daya untuk melakukan perhitungan. Karena didasarkan pada persamaan matematis, AES dapat dengan mudah dibuktikan keamanannya.

METODE PENELITIAN

Metode penelitian yang digunakan adalah penelitian studi literatur dengan metode eksperimen algoritma *Advanced Standard Encryption* (AES). Langkah-langkah peneltian yang dilakukan adalah sebagai berikut:

a. Studi Literatur, tahap ini dilakukan dengan mencari sumber referensi berupa buku, jurnal ilmiah, atau hasil penelitian terdahulu yang terkait dengan algoritma *Advanced Standard Encryption* (AES).
b. Proses Enkripsi dan Deskripsi Proses, proses enkripsi dan dekripsi dilakukan menggunakan *Advanced Standard Encryption* (AES) dengan kunci K=128. Proses

enkripsi adalah proses penyembunyian data dengan cara mengubah dari *plaintext* ke *ciphertext*. Sedangkan proses deskripsi adalah kebalikannya, proses pengembalian dari *ciphertext* menjadi *plaintext* kembali. Tujuannya adalah untuk memahami pesan yang ada sehingga pengguna dapat membacanya dengan benar.

c. Kesimpulan, kesimpulan hasil pengujian didapatkan setelah proses enkripsi dan dekripsi menggunakan *Advanced Standard Encryption* (AES) berhasil dilakukan.

Dari langkah-langkah tersebut dijadikan landasan untuk membuat penelitian ini agar terlaksana dengan baik.

HASIL DAN PEMBAHASAN

Misalkan seseorang akan mengirim sebuah plainteks yang berisi 128bit atau 16*byte* atau 16 karakter seperti berikut:

Plainteks: *Kriptografi AES* dengan Kunci: *Aditia*

Maka plainteks ini dapat dibuat menjadi state berikut:

Plainteks : Kunci :

K	t	a	A
R	o	f	E
I	g	i	S
P	r	(spase)	(null)

Tabel 1. 1 Transposisi plainteks

A	i	(null)	(null)
D	a	(null)	(null)
I	(null)	(null)	(null)
T	(null)	(null)	(null)

Tabel 1. 2 Transposisi kunci

Pada AES menggunakan representasi byte bilangan heksaadesimal. Maka karakter teks di atas dikonversi menjadi bilangan heksaadesimal dengan melihat table KODE ASCII maka didapat seperti berikut:

Plainteks :

4B	74	61	41
72	6F	66	45
69	67	69	53
70	72	20	00

Tabel 1. 3 Konversi heksadesimal plainteks

Kunci :

41	69	00	00
64	61	00	00
69	00	00	00
74	00	00	00

Tabel 1. 4 Konversi heksadesimal kunci

Proses Ekspansi Kunci

Proses ekspansi kunci seperti berikut:

41	69	00	00
64	61	00	00
69	00	00	00
74	00	00	00

Atau dapat ditulis

W_0= 41 64 69 74

W_1= 69 61 00 00

W_2= 00 00 00 00

W_3= 00 00 00 00

Tabel 1. 5 Ekspansi kunci

Sehingga untuk mencari W_4 adalah seperti berikut

W_4 $= W_0 \oplus subword\ (rotword\ (W_3)) \oplus RC[1]$

$=41\ 64\ 69\ 74 \oplus subword\ (rotword\ (00\ 00\ 00\ 00)) \oplus 01\ 00\ 00\ 00$

$= 41\ 64\ 69\ 74 \oplus subword\ (00\ 00\ 00\ 00) \oplus 01\ 00\ 00\ 00$

$=23\ 07\ 0A\ 17$

Hasil perhitungan untuk ekspansi untuk 1 *round* terdapat pada *table* seperti berikut ini:

W(i)	***W(i-1)***	***After subword ⊕ rcon ⊕ W(i-NK)***
W4	00 00 00 00	23 07 0A 17
W5	23 07 0A 17	4A 66 0A 17
W6	4A 66 0A 17	4A 66 0A 17
W7	4A 66 0A 17	4A 66 0A 17

Tabel 1. 6 Hasil perhitungan ekspansi

Proses Enkripsi

Langkah pertama yang harus dilakukan adalah Melakukan xor antara plainteks dan kunci, seperti berikut:

4B	74	61	41
72	6F	66	45
69	67	69	53
70	72	20	00

⊕

41	69	00	00
64	61	00	00
69	00	00	00
74	00	00	00

=

0A	1D	61	41
16	0E	66	45
00	67	69	53
04	72	20	00

Tabel 1. 7 Proses Enkripsi Plainteks **Tabel 1. 8 Proses Enkripsi Kunci**

Tabel 1. 9 Hasil Enkripsi

***Round* 1**

Hasil Proses *Subbyte* (menggunakan *table s-box*)

67	A4	EF	83
47	AB	33	6E
63	85	F9	ED
F2	40	B7	63

Tabel 1. 10 *Subbyte*

Transformasi *ShiftRows*

67	A4	EF	83
47	AB	33	6E
63	85	F9	ED
F2	40	B7	63

ShiftRows →

67	A4	EF	83
AB	33	6E	47
F9	ED	63	85
63	F2	40	B7

Tabel 1. 11 Tranformasi *shiftrows* **Tabel 1. 12 Hasil tranformasi *shiftrows***

Proses *MixColumns*

Proses ini merupakan proses yang paling kompleks dari pada proses yang lain di setiap *rounde*. Penulis membagi proses *mixcolumns* menjadi 4 bagian untuk sebuah matriks atau *state* karena dikerjakan untuk setiap kolom sebagai berikut:

Proses *mixcolumn* untuk kolom pertama

$$\begin{bmatrix} S'(0,1) \\ S'(1,1) \\ S'(2,1) \\ S'(3,1) \end{bmatrix} = \begin{bmatrix} 02 & 03 & 01 & 01 \\ 01 & 02 & 03 & 01 \\ 01 & 01 & 02 & 03 \\ 03 & 01 & 01 & 02 \end{bmatrix} * \begin{bmatrix} 67 & A4 & EF & 83 \\ AB & 33 & 6E & 47 \\ F9 & ED & 63 & 85 \\ 63 & F2 & 40 & B7 \end{bmatrix}$$

$$= \begin{bmatrix} B2 & 19 & 54 & E6 \\ 59 & 1C & B8 & 2E \\ 80 & 5B & 87 & 17 \\ 3D & D6 & A7 & 29 \end{bmatrix}$$

Pada *round* pertama didapat Cipherteks yang akan digunakan untuk *input round* 2, begitu juga cipherteks yang didapat pada *round* 2 kan digunakan untuk *input* pada *round* 3. Proses seperti ini berlangsung hingga *round* 10. Pada *round* 10 didapat hasil enkripsi sebagai berikut:

Round-10:

Sub-byte =

D9	36	01	59
EE	D4	FF	36
EF	AD	D1	AE
2B	B7	BC	56

Tabel 1. 13 *Subbyte round-10*

Shift Rows =

D9	36	01	59
D4	FF	36	EE
D1	AE	EF	AD
56	2B	B7	BC

Tabel 1. 14 *Shift Rows round-10*

Addround key =

9A	79	9E	64
53	8C	31	C2
F4	99	B6	38
59	64	64	68

Tabel 1. 15 *Addround Key Round-10*

Pada round 10 transformasi dilakukan hanya 3 transformasi yaitu *Subbyte*, *ShiftRows,Addroundkey.* Dan didapat cipherteks yang sesungguhnya yaitu:

Cipherteks =

9A	79	9E	64
53	8C	31	C2
F4	99	B6	38
59	64	64	68

Tabel 1. 16 *cipherteks round-10*

Jika didalam bentuk ASCII maka di dapat cipherteks: **š S ô Y y Œ ™ d ž 1¶ d d Â 8 h**

Untuk mengembalikan ciphertext menjadi plaintext, proses dekripsi dilakukan menggunakan transformasi invers dari semua transformasi dasar yang digunakan dalam algoritma enkripsi AES. . Setiap transformasi dasar AES memiliki transformasi invers, yaitu L: *invsubbytes, invshiftrows,* dan *invmixcolumns.* Dari proses dekripsi yang dilaksanakan 10 round didapat:

Plainteks =

4B	74	61	41
72	6F	66	45
69	67	69	53
70	72	20	00

Tabel 1. 17 Hasil dekripsi

Plainteks yang di konversi menjadi bentuk ASCII menjadi: “Kriptografi AES”. Maka pada Algoritma kriptografi AES untuk Plainteks= “Kriptografi AES” dan kunci= “Aditia” didapat Cipherteks= **“š S ô Y y Œ ™ d ž 1¶ d d Â 8 h”.**

KESIMPULAN

Proses enkripsi teks pada algoritma krpitografi AES 128, plainteks terlebih dahulu dikonversi menjadi kode ASCII dalam bilangan hexadesimal dan dibentuk sebagai matriks byte yang berukuran 4x4 yang disebut state. Dalam algoritma AES 128 proses enkripsi merupakan transformasi terhadap state yang dilakukan secara berulang dalam 10 round. Pemrosesan data pada setiap round menggunakan data biner. Setiap round

AES membutuhkan satu kunci hasil generasi kunci dan menggunakan 4 transformasi dasar yaitu subbyte, shifrows, mixcoloumns, dan addroundkey. Sedangkan pada proses deskripsi mempunyai transformasi dengan urutan invshiftrows, invshiftrows, invsubbytes, addroundkey, serta invmixcoloumns.

Enkripsi dan deskripsi dilakukan pada file dokumen yang telah dikonfirmasi memiliki jumlah karakter total lebih dari 16 karakter. Jadi enkripsi dan dekripsi AES dilakukan secara paralel. Sedangkan untuk file teks dengan jumlah karakter kurang dari 16 akan dilakukan padding. Padding adalah penggunaan karakter ASCII null untuk mengisi jumlah karakter yang hilang agar dapat diproses dan tidak mempengaruhi pengkodean atau deskripsi yang dihasilkan.

DAFTAR REFERENSI

Asiyanik. (2017). Studi Terhadap Advanced Encryption Standard (Aes) DanAlgoritma Knapsack Dalam Pengamanan Data. Santika, 7(Jurnal Ilmiah Sains dan Teknologi), 553–561.

Mulyadi, A. Y., Nugroho, E. P., & P, R. R. J. (2018). Implementasi Algoritma AES 128 dan SHA – 256 Dalam Pengkodean pada Sebagian Frame Video CCTV MPEG-2. JATIKOM: Jurnal Teori Dan Aplikasi Ilmu Komputer, 1(1), 33–39.

Nasution, Ainun Haviza, D. (2020). E-Security di dalam Digital Signature Berbasis Algoritma AES (Advanced Encryption Standrt) 128 Bit Pada Slip Gaji Pegawai di Kantor Walikota Medan. Sains Dan Komputer (SAINTIKOM), 21(1), 1–9.

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

Primartha Rifkie. (2011). Penerapan Enkripsi dan Dekripsi File Menggunakan Data Encryption Standard (DES). ISNN : 2355-4614 / Universitas Sriwijaya, 3(2), 371–387.

Azhari, M., Mulyana, D. I., Perwitosari, F. J., & Ali, F. (2022). Implementasi Pengamanan Data pada Dokumen Menggunakan Algoritma Kriptografi Advanced Encryption Standard (AES). Jurnal Pendidikan Sains Dan Komputer, 2(01), 163–171. https://doi.org/10.47709/jpsk.v2i01.1390

Nuari, R., & Ratama, N. (2020). Implementasi Algoritma Kriptografi AES (Advanced Encryption Standard) 128 Bit Untuk Pengamanan Dokumen Shipping. Journal Of Artificial Intelligence And Innovative Applications, 1(2), 2716–1501. http://openjournal.unpam.ac.id/index.php/JOAIIA

Prayudha, J., _ S., & _ I. (2019). Implementasi Keamanan Data Gaji Karyawan Pada PT. Capella Medan Menggunakan Metode Advanced Encryption Standard (AES). Jurnal SAINTIKOM (Jurnal Sains Manajemen Informatika Dan Komputer), 18(2), 119. https://doi.org/10.53513/jis.v18i2.150

Putra, Y., Yuhandri, Y., & Sumijan, S. (2021). Meningkatkan Keamanan Web Menggunakan Algoritma Advanced Encryption Standard (AES) terhadap Seragan Cross Site Scripting. Jurnal Sistim Informasi Dan Teknologi, 3, 56–63. https://doi.org/10.37034/jsisfotek.v3i2.44

Setti, S., Gunawan, I., Damanik, B. E., Sumarno, S., & Kirana, I. O. (2020). Implementasi Algoritma Advanced Encryption Standard dalam Pengamanan Data Penjualan Ramayana Department Store. JURIKOM (Jurnal Riset Komputer), 7(1), 182. https://doi.org/10.30865/jurikom.v7i1.1960

Daemen, J., & Rijmen, V. (2002). "The Design of Rijndael: AES - The Advanced Encryption Standard." Springer. ISBN: 978-3-540-42580-4.

Schneier, B. (1996). "Applied Cryptography: Protocols, Algorithms, and Source Code in C." John Wiley & Sons. ISBN: 978-0471117094.

Ferguson, N., Schneier, B., & Kohno, T. (2010). "Cryptography Engineering: Design Principles and Practical Applications." John Wiley & Sons. ISBN: 978-0470474242.

Delfs, H., & Knebl, H. (2007). "Introduction to Cryptography: Principles and Applications." Springer. ISBN: 978-3540492436.

Menezes, A. J., van Oorschot, P. C., & Vanstone, S. A. (1996). "Handbook of Applied Cryptography." CRC Press. ISBN: 978-0849385230.