Jurnal Riset Sains dan Teknologi
Volume 4 No. 1 Maret 2020, 41 – 46
e-ISSN: 2549-9750
p-ISSN: 2579-9118

Modifikasi Enkripsi dan Dekripsi AES dengan Polybius Chiper dalam Pengamanan Data

Modification Encyprtion and Decryption of AES with Polybius Chiper in Data Security

Shinta Permatasari[1], Aminudin[2*], Sofyan Arifianto[3]
[1,2,3)]Prodi Informatika, Fakultas Teknik
Universitas Muhammadiyah Malang
Jl. Raya Tlogomas No. 246 Malang, Jawa Timur
email: [1]thashinta@webmail.umm.ac.id, *[2]aminudin2008@umm.ac.id , [3]sofyan.arfianto@gmail.com

DOI;
10.30595/jrst.v4i1.6208

Histori Artikel:

Diajukan:
23/12/2019

Direvisi:
12/03/2020

Diterima:
20/03/2020

ABSTRAK

Data merupakan file yang dapat bersifat rahasia sehingga membutuhkan sebuah proses pengamanan data untuk menjaga kerahasiaannya. Kripotgrafi yaitu proses pengamanan data yang dapat digunakan berdasarkan penggunaan algoritma salah satunya AES. AES adalah algoritma modern yang dapat dimodifikasi untuk meningkatkan konfusi dan difusi dalam kriptografi. Kombinasi AES dapat dilakukan menggunakan *Polybius* yang memiliki sifat difusi kriptografi. Penelitian ini melakukan modifikasi AES menggunakan matriks Polybius berukuran 6x6 dan 10x10 yang dilakukan pada plainteks maupun plainteks dan kunci. Analisa dilakukan berdasarkan tingkat perubahan bit tertinggi yang terdapat pada modifikasi II pada plainteks dan kunci matriks 6x6 yaitu sebesar 51,8% menggunakan uji *avalanche effect.* Hasil dari AE dibandingkan dengan hasil yang diharapkan menggunakan *chi square* dengan hasil AES modifikasi dapat meningkatkan *AE* sebesar 5% dengan taraf nyata 0,05 dan derajat kebebasan 4. Waktu eksekusi diuji pada penelitian ini dengan hasil eksekusi waktu AES modifikasi lebih lama dibandingkan AES standar dikarenakan kompleksitas dari algoritma mempengaruhi waktu enkripsi maupun dekripsi.

Kata Kunci: AES, *polybius,* konfusi, difusi

ABSTRACT

Data is a file that can be confidential so it requires a data security process to maintain confidentiality. Kripotgrrafi is a data security process that can be used based on the use of algorithms, one of which is AES. AES is a modern algorithm that can be modified to improve confusion and diffusion in cryptography. AES combination can be done using Polybius which has cryptographic diffusion properties. This study modified the AES using 6x6 and 10x10 polybius matrices that were performed on plaintext and plaintext and keys. Analysis was carried out based on the highest bit change rate found in modification II in the plaintext and 6x6 matrix keys, which amounted to 51.8% using the avalanche effect test. The results of the AE compared to the expected results using chi square with the modified AES results can increase the AE by 5% with the real level is 0,05 and the degree of freedom is 4 . Execution time was tested in this study with the results of the AES modification time longer than the standard AES because the complexity of the algorithm affects both encryption and decryption time.

Keywords : AES, *polybius, confusion, diffusion*

1. PENDAHULUAN

Teknologi pada era ini memungkinkan manusia dapat bertukar informasi berupa data. Data yang dimiliki dapat bersifat rahasia sehingga membutuhkan suatu pengamanan data. Kriptografi merupakan ilmu yang digunakan dalam peroses pengamanan data berdasarkan algoritma atau metode yang digunakan.

AES merupakan algoritma kriptografi modern yang banyak digunakan karena dianggap aman dan efisien. AES 128 bit memiliki ruang kunci 2^{128} yang dianggap aman dan terhindar dari sengan *bruteforce attack* (Tulloh, Permanasari, & Harahap, 2016) . Serangan terhadap sebuah algoritma dapat menyebabkan proses pengamanan data dinyatakan lemah. Penelitian (Des, Algoritma, Dalam, & File, 2014) menyatakan kelemahan yang dapat timbul dalam algoritma AES yaitu kompleksitas pada *chipper block* sehingga peningkatan konfusi dan difusi sangat penting.

Konfusi dan difusi merupakan konsep kriptografi yang bertujuan untuk mengaburkan pola statistic antara plainteks, chiperteks dan kunci. Modifikasi AES dapat dilakukan menggunakan *polybius chipper* yang memiliki fraksionasi yaitu mengarah kepada konsep kriptografi (Kondo & Mselle, 2013). Penelitian (Kumar & Rana, 2016) melakukan modifikasi menggunakan matriks 6x6 dengan hasil penelitian terfokus pada proses eksekusi enkripsi dan dekripsi yang membutuhkan waktu yang lebih lama. Penelitian (Rahman et al., 2016) melakukan modifikasi AES dan RSA berdasarkan plainteks dan kunci menggunakan *polybius* dengan perluasan matriks 9x9.

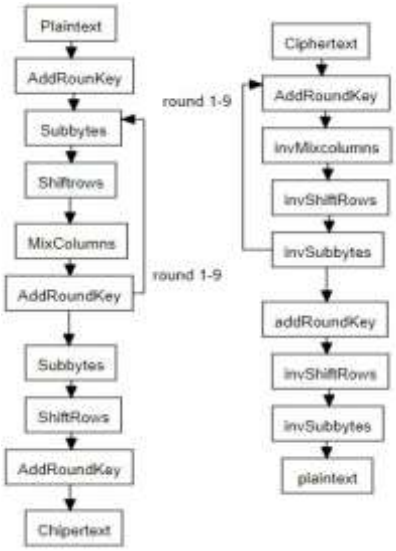
Penelitian ini melakukan modifikasi AES menggunakan *Polybius chipper* pada plainteks dan kunci dengan penggunaan matriks 6x6 dan perluasan matriks 10x10 untuk menguji performa waktu enkripsi, dekripsi dan mengukur tingkat perubahan bit sehingga dapat dianalisa kekuatan dari sebuah algoritma.

2. METODE PENELITIAN

AES melakukan beberapa transformasi pada proses enkripsi yaitu AddRoundkey, Subbytes, ShiftRows dan MixColumn. Dekripsi dilakukan dengan invers dari setiaptransformasi pada proses enkripsi yaitu Invers Subbytes, invers shiftrows, invers mixcolumn. Proses Key Expansion dilakukan sama baik pada proses enkripsi maupun dekripsi. Hasil dari key expansion berupa kunci yang akan digunakan untuk setiap putaran pada transformasi selanjutnya.

2.1 Algoritma AES

Proses enkripsi merupakan proses perubahan plainteks menjadi chiperteks sehingga isi dari file menjadi acak. Algoritma AES-128 bit digunakan pada penelitian ini dengan jumlah putaran 10 . Proses enkripsi dan dekripsi memiliki satu kunci untuk melakukan proses pengamanan data. Hasil enkripsi berupa symbol yang tidak dapat dibaca kembali dikarenakan penggunaan beberapa transformasi yang membuat proses konfusi dan difusi pada algoritma AES. Hasil enkripsi berupa chiperteks akan menghasilkan bentuk plainteks dengan isi file semula sehingga isi file dapat dibaca kembali. Alur kerja proses enkripsi dan dekripsi dapat dilihat pada flowchart Gambar 1.



Gambar 1. Enkripsi dan Dekripsi AES

Transformasi pertama dilakukan proses addroundkey yang merupakan putaran ke-0 kemudian melakukan proses transformasi pertama yaitu *subbytes* melakukan subtitusi menggunakan tabel S-Box, *shiftrows,* melakukan pergeseran ke kiri berdasarkan indeks baris, *mixcolumn* melakukan proses penjumlahan dan perkalian pada GF 2^8 dan *Key Expansion* melakukan proses pembangkitan kunci yang menghasilkan kunci untuk digunakan disetiap transformasi.

Berdasarkan Gambar 1 proses awal dekripsi dilakukan sama dengan proses enkripsi yaitu AddRoundKey dengan melakukan proses transformasi selanjutnya yaitu *invers subbytes* yaitu melakukan subtitusi menggunakan tabel invers S-box, *invers shiftrows* yaitu pergeseran ke kanan sesuai dengan index baris, *mixcolumn* yaitu melakukan proses penjumlahan dan perkalian matriks menggunakan tabel ketetapan RCon inv mixcolumn dan melakukan proses pembangkitan kunci untuk setiap putaran.

2.2 Algoritma Modifikasi

Polybius square digunakan untuk proses modifikasi pada tahap awal baik pada modifikasi plainteks maupun pada modifikasi plainteks dan kunci. Modifikasi dilakukan sebelum proses transformasi yang terdapat pada algoritma AES standar dengan menggunakan matriks berukuran 6x6.

	0	**1**	**2**	**3**	**4**	**5**
0	a	b	c	d	e	f
1	g	h	i	j	k	l
2	m	n	o	p	q	r
3	s	t	u	v	w	x
4	y	z	1	2	3	4
5	5	6	7	8	9	

Gambar 2. Matriks 6x6

Proses subtitusi dilakukan berdasarkan karakter yang digunakan pada plainteks maupun kunci berdasarkan indeks baris kemudian kolom. Setelah melakukan proses subtitusi matriks selanjutnya melakukan proses transformasi pada AES yaitu *addroundkey, subbytes, shitrows, mixcolumn* dan *key expansion.* Proses dekripsi dilakukan sama namun dengan penambahan proses subtitusi pada awal dekripsi kemudian melakukan transformasi yang terdapat pada proses dekripsi AES standar. Penelitian ini menggunakan matriks kedua yaitu 10x10 untuk mengetahui tingkat perubahan bit yang dihasilkan dari setiap modifikasi sesuai pada Gambar 3.

	0	1	2	3	4	5	6	7	8	9
0	a	b	c	d	e	f	G	h	i	j
1	k	l	m	n	o	p	q	r	s	t
2	u	v	w	x	y	z	0	1	2	3
3	4	5	6	7	8	9		!	@	#
4	$	%	^	&	*	(	)	-	+	(
5	)	_	=	[	]	;	"	.	,	?
6	<	>	:	'	/	\	α	β	γ	δ
7	ε	∀	η	θ	λ	μ	∩	σ	Φ	
8	∫	Ã	Ẽ	÷	≠	¥	≤	≥	↓	→
9	←	↑	↔	¶	∑	Ω	|	∅	Δ	~

Gambar 3. Matriks 10x10

Modifikasi 1 dilakukan berdasarkan perubahan plainteks menggunakan masing-masing matriks Polybius. Modifikasi 2 dilakukan berdasarkan perubahan plainteks dan kunci yang disubtitusikan menggunakan masing-masing matriks polybius pada Gambar 2 dan 3 sehingga menghasilkan 4 modifikasi dengan penggunaan matriks yang berbeda. Penggunaan matriks akan mempengaruhi hasil dari masing-masing pengujian yang digunakan.

2.3. Metode Pengujian

Pengujian yang dilakukan menggunakan metode pengujian *avalanche effect*. Pengujian tersebut mengukur tingkat perubahan bit yang dapat dianalisa berdasarkan masing-masing algoritma standar dan modifikasi. Rumus yang digunakan sesuai pada persamaan 1.

$$AE = \frac{total\ perubahan\ bit}{total\ keseluruhan\ bit} * 100\% \qquad (1)$$

Semakin tinggi nilai persentase dari hasil pengujian , maka algoritma dapat dikatakan baik sehingga aman dari kriptoanalis (Salim, 2017). Pengujian lain juga digunakan untuk menguji hasil pengujian sebelumnya dengan hasil yang diharapkan sehingga dapat menentukan apakah kedua hasil berbeda secara signifikan (Salim, 2017). Penelitian menggunakan taraf nyata 0,05 dengan derajat kebebasan 4. Hasil hipotesis didapatkan berdasarkan persamaan 2.

$$X^2 = \sum_{i=1}^{n} \frac{(O_i - E_i)^2}{E_i} \qquad (2)$$

Apabila hasil nilai hitung < dibandingkan nilai tabel chi square maka hipotesa 1 diterima dan hipotes 2 ditolak begitu

pula sebaliknya. H0 merupakan hipotesis awal yang digunakan yaitu AES modifikasi dapat meningkatkan avalanche effect sebesar 5% dan H1 merupakan hipotesis alternative yang menolak hipotesis awal yaitu AES modifikasi TIDAK dapat meningkatkan avalanche effect sebesar 5%.

Performa algoritma kriptografi juga meliputi proses waktu enkripsi dan dekripsi sehingga dapat mengetahui kecepatan proses dalam pengamanan data apabila memiliki ukuran *file* yang besar.

2.4. Pengacuan Pustaka

Pengacuan skenario didasari beberapa hal yaitu mengacu pada pengujian Avalanche effect, Chi Square dan performa waktu.

1. Avalanche effect

Pengujian AE dilakukan untuk mengetahui perubahan bit berdasarkan rumus 1 yang didasari penelitian (Rumani, 2015) yang merepresentasikan perbandingan perhitungan AE untuk setiap modifikasi AES. Hasil penelitian menunjukkan AES dapat diterapkan pada aplikasi chat dengan tingkat *avalanche effect* yang tinggi yaitu mencapai 90%.

2. Chi Sqaure

Pengujian ini dilakukan untuk membandingkan hasil pengujian AE dengan hasil yang diharapkan yang didasari pada penelitian (Salim, 2017) yang melakukan penelitian modifikasi AES menggunakan *Chaotic Blum-blum.* Penelitian ini melakukan uji chi square dengan parameter AE dan performa waktu menggunakan taraf nyata 0,05. Hasil menunjukkan bahwa hipotesa awal diterima yaitu AES modifikasidapat meningkatkan *avalanche effect* sebesar 5%.

3. Performa waktu

Pengujian performa waktu mengacu pada penelitian (Suartana, 2019) melakukan analisa waktu eksekusi enkripsi dan dekripsi. Hasil penelitian melukukan peningkatan jumlah putaran dengan hasil eksekusi waktu AES modifikasi lebih tinggi dibandingkan dengan AES standar. Semakin lama waktu eksekusi maka memiliki tingkat keamanan yang semakin tinggi.

3. HASIL DAN PEMBAHASAN

Hasil dapat dianalisa berdasarkan tiga metode pengujian yaitu *avalanche effect, chi square* dan eksekusi waktu.

3.1 *Avalanche effect*

Pengujian dilakukan berdasarkan indeks rumus 1 sehingga mendapatkan hasil seperti terlihat pada Tabel 1 berikut.

Tabel 1. Hasil pengujian *avalanche effect*

No	Algoritma	Avalanche Effect
1	AES Standar	46,2%
2	AES modifikasi I pada plain 6x6	51,2%
3	AES modifikasi I pada plain 10x10	50,6%
4	AES modifikasi II pada plain dan key 6x6	
5	AES modifikasi II pada plaindan key 10x10	50,8%

Tingkat avalanche effect rendah pada algoritma AES standar sedangkan tertinggi terdapat pada AES modifikasi II pada plain dan kunci matriks 6x6. Perubahan bit tertinggi didapatkan dari hasil modifikasi sehingga subtitusi karakter pada penggunaan matriks dalam modifikasi mempengaruhi tingkat perubahan bit. Hasil didapatkan berdasarkan rata-rata dari 5 uji file yang sama, Hasil

3.2 *Chi square*

Pengujian ini dilakukan mengacu pada data hasil pengujian sebelumnya. Hipotes pertama yang digunakan yaitu AES modifikasi dapat meningkatkan *avalanche effect* sebesar 5% dan hipotesa kedua yaitu AES modifikasi TIDAK dapat meningkatkan *avalanche effect* sebesar 5%. Hasil didapatkan berdasarkan Tabel 2 berikut .

Tabel 2. Hasil pengujian chi square

No	Param	Tn	Db	Ci tabel	x^2	Hasil
1	AE modif I 6x6	0,05	4	9,4877	0,5859	H0 diterima
2	AE modif I 10x10	0,05	4	9,4877	1,0647	H0 diterima
3	AE modif II 6x6	0,05	4	9,4877	1,3407	H0 diterima
4	AE modif II 10x10	0,05	4	9,4877	1,022	H0 diterima

Tabel 2 menunjukkan hasil pengujian dengan taraf nyata 0,05 dan derajat kebebasan 4. Nilai dari chi square table dilihat berdasarkan

taraf nyata dan db yang digunakan. Hasil menunjukkan H0 diterima dan H1 ditolak sehingga didapatkan kesimpulan AES modifikasi dapat meningkatkan *avalanche effect* sebesar 5%.

3.3 Performa Waktu

Implementasi perfoma waktu dilakukan berdasarkan proses enkripsi dan dekripsi. Hasil akan menunjukan waktu yang dibutuhkan untuk melakukan proses enkripsi dan dekripsi berdasarkan ukuran file yang berbeda. Proses enkripsi lebih cepat akan lebih baik karena membutuhkan waktu yang relative singkat tetapi prses derkipsi lebih lama akan lebih baik karena membutuhkan waktu untuk mengetahui kunci yang digunakan da;am proses pengacakan. Hasil dapat dilihat bersarkan Tabel 3 berikut .

Tabel 3. Hasil pengujian waktu enkripsi

Size File	AES	AES modif I 6x6	AES modif I 10x10	AES modif II 6x6	AES modif II 10x10
11kb	195	465	534	409	658
12kb	790	1458	2251	1439	1884
13kb	3991	7620	7667	8639	10124
14kb	5530	9886	12628	9951	12473
15kb	6450	12006	14733	12118	13782
Rata-rata	3391,2	6287	7562,6	6511,2	7784,2

Hasil menunjukkan bahwa AES standar memiliki performa waktu yang baik. Hal ini dikarenakan adanya penambahan matriks pada proses pengamanan data sehingga waktu yang dibutuhkan relative lama. Hasil dapat dilihat bersarkan Tabel 4 berikut .

Tabel 4. Hasil pengujian waktu dekripsi

Size File	AES	AES modif I 6x6	AES modif I 10x10	AES modif II 6x6	AES modif II 10x10
11kb	260	608	1726	542	863
12kb	1145	2404	2961	2569	3208
13kb	6399	10992	14564	11544	16851
14kb	8913	15194	19539	15144	18183
15kb	10000	20174	22400	18862	22400
Rata-rata	5502,6	9874,4	12238	9732,2	12301

Hasil menunjukkan bahwa AES modifikasi memiliki performa watku yang baik. Hal ini dikarenakan proses subtitusi yang digunakan dapat mempengaruhi waktu eksekusi sehingga membutuhkan waktu yang relative lebih lama dalam melakukan pengacakan kunci.

4. KESIMPULAN

Algoritma dilakukan pengujian *avalanche* effect dengan persentase tertinggi terdapat pada algoirtma modifikasi menggunakan matriks 6x6 pada plainteks dan kunci yaitu sebesar 51,8% yang berarti perubahan bit terbanyak terdapat pada algoritma modifikasi dengan hasil pengujian chi square yang menunjukkan AES modifikasi yang digunakan dapat meningkatkan *avalanche effecti* sebesar 5%. Performa waktu enkripsi dan dekripsi yang dimiliki untuk masing-masing AES modifikasi membutuhkan waktu yang relative lama dibandingkan AES standar dikarenakan komplekasitas algoritma yang digunakan mempengaruhi waktu komputasi.

DAFTAR PUSTAKA

Des, T., Algoritma, D. A. N., Dalam, A. E. S., & File, P. (2014). *Konferensi Nasional Ilmu Komputer (KONIK) 2014 KOMBINASI ALGORITMA TRIPLE DES DAN ALGORITMA AES DALAM PENGAMANAN FILE*. (July 2016).

Kondo, T. S., & Mselle, L. J. (2013). *An Extended Version of the Polybius Cipher*. *79*(13), 30–33.

Kumar, P., & Rana, S. B. (2016). Development of modified AES algorithm for data security. *Optik*, *127*(4), 2341–2345. https://doi.org/10.1016/j.ijleo.2015.11.188

Rahman, Z., Science, M. B., Corraya, A. D., Science, M. B., Sumi, M. A., & Science, M. B. (2016). *A Novel Structure of Advance Encryption Standard (AES) with 3-Dimensional S- box , RSA based Key Scheduling and modified 3-Dimensional Polybius Cube Encipherment A Novel Structure of Advance Encryption Standard (AES) with*. (February 2017), 0–8.

Rumani, R. (2015). Desain Dan Implementasi Aplikasi Sms (Short Message Service) Pada Android Menggunakan Algoritma Aes. *E-Proceeding of Engineering*, *2*(2),

3318–3326.

Salim, M. A. (2017). *Analisa Algoritma AES Modifikasi dengan Teknik Blum Blum Shub - Chaotic Function dan Modifikasi ShiftRows*. 1–79.

Suartana, I. M. (2019). *Implementasi Kriptografi dengan Modifikasi Algoritma Advanced Encryption Standard (AES) untuk Pengamanan File Document*. *01*(November 2001), 42–47.

Tulloh, A. R., Permanasari, Y., & Harahap, E. (2016). Kriptografi Advanced Encryption Standard (AES) Untuk Penyandian File Dokumen. *Jurnal Matematika UNISBA*, *2*(1), 118–125.