ANALISIS KINERJA ALGORITMA ADVANCED ENCRYPTION STANDARD (AES) TERMODIFIKASI DALAM ENRKIPSI DAN DEKRIPSI DATA

(PERFORMANCE ANALYSIS OF MODIFIED ADVANCED ENCRYPTION STANDART (AES) ALGORITHM FOR ENCRYPTING AND DECRYPTING DATA)

Candra Aditya Pinuyut [1)], Ema Utami [2)], dan Alva Hendi Muhammad[3)]
[1, 2,3)] Magister Teknik Informatika, Universitas Amikom Yogyakarta
Yogyakarta, Indonesia
e-mail: candra@students.amikom.ac.id[1)], ema.u@amikom.ac.id[2)], alva@amikom.ac.id [3)]

ABSTRAK

Advanced Encryption Standard (AES) adalah salah satu algoritma enkripsi yang paling populer digunakan saat ini. Keamanan data semakin penting dalam era digital ini, sehingga diperlukan penelitian untuk meningkatkan kinerja algoritma enkripsi. Penelitian ini bertujuan untuk menganalisis kinerja algoritma Advanced Encryption Standard (AES) yang telah dimodifikasi dalam proses enkripsi dan dekripsi. Fokus utama penelitian ini adalah mengukur nilai Avalanche Effect, throughput, dan kecepatan proses enkripsi serta dekripsi dari AES termodifikasi. Modifikasi dilakukan dengan mengganti fungsi mixcolumn dengan bit permutasi dan mengurangi jumlah putaran terhadap algoritma AES konvensional. Perbandingan dilakukan antara AES termodifikasi dengan algoritma AES standar, Twofish, Serpent, DES, dan 3DES. Pengujian meliputi pengukuran Avalanche Effect, throughput, dan kecepatan enkripsi serta dekripsi. Hasil penelitian menunjukkan bahwa algoritma AES termodifikasi memiliki Avalanche Effect sebesar 50.20%, lebih tinggi dibandingkan dengan algoritma AES konvensional yang memiliki Avalanche Effect 49.63%. Pengujian throughput menunjukkan bahwa AES termodifikasi tidak mengalami perubahan signifikan dibandingkan algoritma AES standar, Serpent, Twofish, DES, dan 3DES saat proses enkripsi. Namun, terdapat perubahan signifikan pada proses dekripsi sebesar 467.37% dibandingkan DES dan 1286% dibandingkan 3DES. Penelitian ini menunjukkan bahwa modifikasi pada AES dapat meningkatkan keamanan dan efisiensi proses dekripsi, meskipun tidak berdampak signifikan pada throughput proses enkripsi.

***Kata Kunci**: Advanced Encryption Standard (AES) Modifikasi, Analisis Algoritma, Bit Permutation,*

ABSTRACT

The Advanced Encryption Standard (AES) is one of the most widely used encryption algorithms today. In the digital era, data security is becoming increasingly important, necessitating research to improve the performance of encryption algorithms. This study aims to analyze the performance of the modified Advanced Encryption Standard (AES) algorithm in the encryption and decryption process. The primary focus of this research is to measure the Avalanche Effect, throughput, and speed of the encryption and decryption processes of the modified AES. The modification involves replacing the mixcolumn function with bit permutation and reducing the number of rounds in the conventional AES algorithm. A comparison is made between the modified AES and standard AES algorithms, Twofish, Serpent, DES, and 3DES. Testing includes measuring the Avalanche Effect, throughput, and encryption and decryption speeds. The results show that the modified AES algorithm has an Avalanche Effect of 50.20%, higher than the conventional AES algorithm, which has an Avalanche Effect of 49.63%. Throughput testing indicates that the modified AES does not show significant changes compared to the standard AES, Serpent, Twofish, DES, and 3DES algorithms during encryption. However, there is a significant change in the decryption process, with an increase of 467.37% compared to DES and 1286% compared to 3DES. This study demonstrates that modifying AES can enhance security and the efficiency of the decryption process, although it does not significantly impact the throughput of the encryption process.

***Keywords**: : Advanced Encryption Standard (AES) Modification, Algorithm Analysis, Bit Permutation*

I. PENDAHULUAN

Dengan pesatnya kemajuan zaman, bidang ilmu keamanan data juga mengalami perkembangan. Saat ini, istilah kriptografi menjadi populer. Kriptografi secara umum adalah bidang ilmu yang mempelajari metode untuk memastikan bahwa informasi yang dikirimkan dapat sampai kepada penerima dengan keamanan yang terjamin Kriptografi mempelajari tatacara penulisan pesan secara rahasia dengan tujuan bahwa komunikasi dan data dapat sembunyikan

(*encode*) dan dibaca (*decode*) kembali untuk mencegah pihak-pihak lain yang ingin mengetahui isinya. Kriptografi dibedakan menjadi dua yaitu kriptografi simetri dan asimetri. Pada kriptografi simetri, kunci yang sama digunakan dalam proses enkripsi dan deskripsi, sedangkan pada kriptografi asimetri menggunakan kunci yang berbeda dalam proses enkripsi dan deskripsi. Algoritma asimetri yang paling banyak digunakan adalah Advanced Encryption Standard (AES). AES adalah standar enkripsi yang ditetapkan oleh National Institute of Standards and Technology (NIST) dan digunakan secara luas karena keamanan dan efisiensinya. Algoritma ini menggunakan panjang kunci 128, 192, atau 256 bit [1]

AES sebagai algoritma kriptografi yang paling umum digunakan pada perangkat keras dan lunak[2], terdapat masalah dalam komputasi yang lebih tinggi karena proses transformasi *MixColumn* menyebabkan proses enkripsi lambat [3]. modifikasi pada AES dengan mengganti proses *MixColumn* dengan *permutation bit* tersebut diuji coba pada file gambar dengan memberikan hasil yang cukup signifikan, yaitu peningkatan proses enkripsi sebesar 16,8% dan deskripsi sebesar 11.96% [4].

Dalam kriptografi, penekanan terhadap keamanan lebih penting dibandingkan kecepatan, sehingga penting untuk melakukan pengujian lebih lanjut terhadap AES termodifikas. AES termodifikasi memberikan peningkatan terhadap *Avalanche effect* sebesar 16.53% dan *throughput* sebesar 33.73% pada proses enkripsi dan 23.72%[5] pada proses deskripsi, sehingga memberikan kesimpulan bahwa AES termodifikasi aman untuk digunakan.

Akan tetapi, pengujian yang dilakukan pada beberapa penelitian sebelumnya hanya diuji coba pada data yang berukuran kecil, sehingga perlu dilakukan pengukuran kinejra algoritma AES termodifikasi pada ukuran file yang lebih besar. modifikasi AES pada file yang lebih besar, memberikan peningkatan sebesar 18.47% pada sisi enkripsi dan 18.77% pada sisi desrkripsi. Pengujian Avalanche effect yang dilakukan memberikan peningkatan sebesar 16.53%[5].

Adapaun tujuan dari penelitian ini adalah untuk menganalisa kinerja dan efektifitas penggunaan algoritma AES termodifikasi dan algoritma twofish, serpent, AES konvensional, DES dan 3DES pada proses enkripsi dan deskripspi, sehingga bisa memberikan evaluasi secara statistik tentang kinerja dan efektifitas penggunaan AES termodifikasi.

II. STUDI PUSTAKA

AES merupakan salah satu algoritma kriptografi yang banyak digunakan karena penggunaanya yang sangat sederhana. Penelitian yang dilakukan oleh [6]bertujuan untuk membandingkan kinerja Algoritma AES dan RC4. Penilitan tersebut dilakukan menggunakan *CrypTool* 2, salah satu putstaka python yang memberikan banyak fungsi terkait kriptografi. Pengujian yang dilakukan pada penelitian ini fokus pada perbandingan besaran ukuran teks yang terkenkripsi dan derskripsi. Hasilnya, proses enkripsi dan desrkirpsi pada RC4 tidak mengalami perubahan terkait ukuran Byte teks, akan tetapi AES mengalami perubahan bit pada sisi enkripsi dan deskripsi, sehingga dapat disimpulkan, pada penelitian tersebut kinerja RC4 lebih unggul dibandingkan dengan AES [6] Akan tetapi, AES masih bisa ditingkatkan lebih lanjut untuk memperbaikan kinerjan algoritima tersebut [7]

Penelitian yang dilakukan oleh [3] tertulis bahwa, walaupun algoritma AES terkenal dengan kinejranya yang penggunaanya sederhana, terdapat ruang yang bisa disempurnakan untuk meningkatkan kinerjanya[2]. Adapun proses penyempurnaan tersebut bisa dilakukan pada empat fungsi transformasi AES yaitu *SubBytes, ShiftRows, MixColumns*, dan *AddRoundKey*[8]. Penelitian ini melakukan dua perubahan yaitu mengganti *MixColumns* dengan teknik permutasi bit dan mengurangi putaran dari 10 menjadi 6 putaran. Adapun pengujian yang dilakukan pada peniiltian ini terfokus pada modifikasi AES 128 bit. Hasilnya, algoritma AES yang dimodifikas memberikan capaian throughput sebesar 31.12% untuk enkripsi dan 25.50% untuk deskripsi, sedangkan pada AES konvensional memberikan nilai 7.18% untuk enkripsi dan 11.32% pada desrkripsi. Hal ini menunjukan bahwa AES termodifikasi bisa memberikan kinerja dan evektifitas yang baik dibandingkan dengan AES konvensional [3]

Penelitian selanjutnya dilakukan oleh [7] bertujuan untuk membandingkan kinerja algoritma AES dan RSA. Adapun pengujian tersebut dilakukan menggunakan CPU Intel-R core-tm i-7 4510U 2,60-GHz, proses berbasis x64, RAM 12 GB, sistem operasi 64 bit. Pengujian dilakukan pada jumlah kata yang beragam dengan mengukur kecapatan waktu enkripsi dan deskripsi.Pada

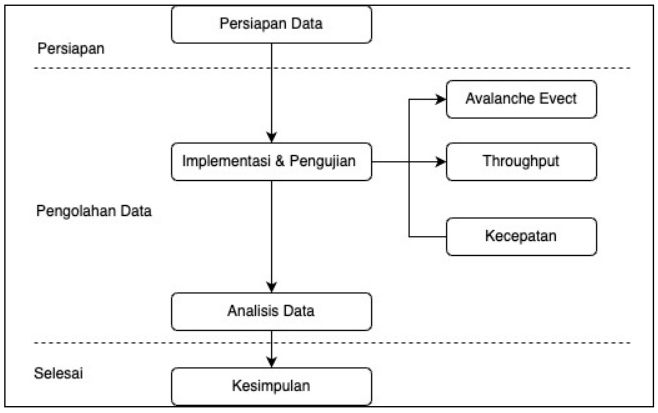
proses enkripsi jumlah kata 100 sampai dengan 5000, AES menghasilkan waktu enkripsi yang lebih cepat dibandingkan dengan RSA. Hal tersebut menunjukan bahwa algoritma AES lebih unggul dibanding RSA dari segi kecepatan [6], [9] Penelitian selanjutnya yang dilakukan oleh [9]melakukan modifikasi terhadap AES dengan mengurangi jumlah putaran pada AES 256 bit dari sebelumnya 14 putaran menjadi 12 putaran dan mengganti proses mixcolumn dengan teknik bit permutation. Adapuan ujicoba dilakukan untuk membandingkan kinerja algoritma AES Konvensional, DES, 3DES, AES Modifikasi dan Twofish. Hasil ujicoba tersebut menunjukan bahwa AES termodifikasi jauh lebih cepat, selanjutnya 3DES, DES,Twofish dan terakhir AES Konvensional. Dari pengujian keamanan menggunakan perhitungan nilai avalanche effect dan throughput AES Termodifikasi memenuhi standar keamanan dengan nilai melebih 50% [9].
Penelitian selanjutnya dilakukan oleh [4] bertujuan untuk melakuan modfikasi pada algoritma AES dalam mengamankan file teks dan gambar. Teknik *Mix Coloumn* menjadi salah satu hambatan terhadap proses komputasi kriptografi AES yang bisa mempengaruhi kecepatan enkripsi dan deskripsi data[10] .Berbeda dengan beberapa penelitian sebelumnya yang melakukan kombinasi antara penguranan jumlah putaran dan permutasi bit, penelitian ini terfokus pada teknik transformasi permutasi bit. Selain itu, penelitian sebelumnya menggunakan teks sebagai data pengujian, pada penelitian ini menggabungkan antara teks dan gambar. Adapun dalam mode *chipper block chaining* menunjkan bahwa AES termodifikasi memberikan kinerja yang lebih cepat sebesar 18,47% pada proses enkripsi dan 18.77% pada proses deskripsip dibandingkan dengan AES konvensional. Selain itu, pengujian avalanche effect yang dilakukan, menunjukan bahwa AES termodifikasi unggul16.53% dibanding AES konvensional. Demikian pula hasil uji coba terhadap histogram, entropi informasi dan kofisien korelasi pixel menunjukan bahwa AES termodifikasi jauh lebih baik dibandingkan dengan AES konvensional. Pada uji coba serangan diferensial dan statistik menunjukan bahwa AES termodifikasi tahan terhadap dua serangan tersebut [4].

Penelitian selanjutnya dilakukan oleh [5] untuk melakukan modifikasi terhadap AES menggunakan teknik permutasi bit dan pengurangan jumlah putaran yang dilakukan untuk mengamankan file-file besar dalam proses pertukaran file. Penelitian ini melakukan proses pengamanan tanpa membatasi tipe file dan ukuran file yang akan dienkripsi, sehingga sangat bermanfaat digunakan oleh organisasi/perusahan dalam proses pengamanan file-file rahasia. Hasilnya pengujian menunjukan bahwa AES termodifikasi mengalami peningkatan sebesar 38.8% pada sisi enkripsip dan 44.86% dari sisi desrkripsi untuk file berukuran sedang hingga besar yang berhasil diuji coba [3].

Berdasarkan peneletian di atas, peneliti akan mengukur kinerja algortima AES termodifikasi, kemudian melakukan analisis statistik untuk mengetahui seberapa besar perubahan yang terjadi terhadap AES yang telah dimodifikasi.

III. METODE PENELITIAN

Penelitian ini dimulai dari melakukan persiapan data, Implementasi dan pengujian, selanjutnya melakukan analisis data dan terakhir melakukan pengambilan kesimpulan terhadap data yang telah dianalisa paa tahap sebelumnya. Adapun alur penelitian seperti pada gambar 1.



Gambat 1. Alur Metode Penelitian

A. *Perispan Data*

Penelitian ini menggunakan data Wajib Pajak Daerah Kota Kotamobagu sebagai sampel pengujian. Adapun data tersebut terdiri dari 130 baris denga tipe data CSV.

B. *Pengukuran Avalanche Effect*

Avalanche Effect merupakan sebuah metode untuk mencari dan mengetahui berapa persen pengubahan pesan pada saat proses enkripsi dilakukan dengan melihat rasio antara jumlah bit dari cipherteks yang berubah dan jumlah bit dari plainteks sebelum dirubah dalam proses enkripsi[11], semakin besar persen yang dihasilkan semakin bagus juga enkripsi yang dihasilkan dan sebaliknya. Pengujian *Avalanche Effect* dianggap

baik apabila terjadi perubahan bit yang menunjukkan antara 45-60% (50 % adalah hasil yang dianggap baik dalam pengujian. Untuk mengurkur Avalanche Effect menggunakan rumus berikut:

$$x = \frac{w}{y} \text{ x } 100 \quad (1)$$

x = Nilai Avalanche Effect
w = Jumlah bit berbeda
y = Total bit

C. Pengukuran Kecepatan

Pengukuran ini memberikan informasi terkait rata-rata waktu yang dibutuhkan oleh algoritma untuk melakukan proses enkripsi dan deskripsi pada 10 kali percobaan.Pengukuran enkripsi/deskripsi dilakukan dengan cara menghitung selisih waktu yang diperlukan oleh algoritma kriptografi sebelum dan sesudah data terenkripsi/terdeskripsi [5].

$$x = w^1 - w^2 \ (2)$$

x = Total selisi waktu
w^1 = Waktu saat enrkipsi/dekripsi selesai
w^2 = Waktu saat enkripsi/dekripsi dimulai

D. Pengukuran Througput

Penilaian kinerja algoritma melalui evaluasi throughput memberikan rekomendasi terhdap kinerja kriptgorafi dalam melakukan proses enkripsi dan deskripsi pada suatu file. Jika nilai thgroughput tinggi, maka algoritma tersebut cocok untuk digunakan dalam proses enkripsi dan deskripsi. Untuk mengukur *throughput*, kita bisa menggunakan rumus berikut [9].

$$x = y - z \ (3)$$

x = *Nilai Throughput enkripsi*
y = *ukuran file*
z = *waktu (ms)*

E. Analisis Data

Data-data yang telah diuji berdasarkan persamaan 1, 2 dan 3, kemudian dibuat menjadi tabel deskriptif. Selanjutnya, berdasarkan tabel deskriptif tersebut, peneliti membuat pengujian menggunakan metode *Dunnett Test* untuk mengukur, apakah terjadi perbedaan kinerja yang signifikan antara AES termodifikasi dan Twofish, Serpent, 3DES, DES.

IV. HASIL DAN PEMBAHASAN

Pada bagian ini, kami melakukan eksperimen dengan melakukan perbandingan terhadap kinerja AES termodifikasi dan algoritma lainya. Adapun AES yang dimodifikasi menghapus fungsi *mixcolumn* pada fungsi AES, kemudian mengganti dengan *bit permutation*. Selain itu, jumlah putaran juga dikurangi dari sebelumnya 14 putaran, menjadi 12 putaran.

Tujuan dari eksperimen ini adalah untuk mengukur, apakah terjadi perbedaan yang signifikan terhadap kinerja AES termodifikasi dan algoritmya kriptografi lainya. Pada penelitian ini kami membandingkan AES termodifikasi dengan AES standart, Twofish, 3DES,DES dan Serpent.

Kami menggunakan eksperimen dengan 100 kali percobaan pada data di atas 1-10 MB. Selanjutnya kami mengambil nilai rata-rata waktu pengujian tersebut seperti pada tabel 1.

Tabel 1. Hasil Pengujian Enkripsi

Algoritma	Kecepatan (detik)
AES	0.001848
Twofish	0.001911
Serpent	0.001917
DES	0.018529
3DES	0.054502
AES Modifikasi	0.001841

Tabel 2. Hasil Pengujian Dekripsi

Algoritma	Kecepatan (detik)
AES	0.001922
Twofish	0.001871
Serpent	0.001896
DES	0.018627
3DES	0.054200
AES Modifikasi	0.001760

Berdasarkan hasil rata-rata waktu enkripsi dan dekripsi, algoritma enkripsi tercepat adalah AES termodifikasi dengan kecepatan rata-rata 0.001841 detik, disusul AES, Twofish, Serpent, DES dan 3DES. Selisih waktu antara AES konvensional dan modifikasi sebesar 0.38%, artinya tidak terdapat selisih yang signifikan antara AES konvensional dan AES standar dari sisi waktu enkripsi.

Selanjutnya, dari proses dekripsi, algortima tercepat adalah adalah AES termodifikasi dengan kecepatan rata-rata 0.001760 detik disusul Twofish, Serpent, AES, DES dan 3DES. Selisih antara AES termodifikasi dan AES standar yaitu 8.43%.

Selanjutnya melakukan analisis ANOVA test terhadap hasil pengujian di atas untuk untuk membandingkan rata-rata dari tiga atau lebih kelompok data yang diuji. Adapun hasil ANOVA test terhadap nilai F-statistic 16148.84 dan F-Value 0.0. Nilai p-value sebesar 0.0 menunjukkan bahwa terdapat perbedaan yang sangat signifikan antara rata-rata waktu enkripsi dari algoritma yang diuji. Ini berarti kita dapat menolak hipotesis nol yang

menyatakan bahwa semua algoritma memiliki rata-rata waktu enkripsi yang sama.

Dengan hasil ini, kami melanjutkan melakukan analisis Tukey's HSD test untuk menentukan pasangan algoritma mana yang berbeda secara signifikan dari sisi enkripsi.

Tabel 3. Hasil Tukey's HSD Test proses enkripsi

Group1	Group2	Meandiff	p-adj	Lower	Upper	reject
AES	Modified AES	-0.0000	1.000	-0.0037	0.0037	False
3DES	Modified AES	-0.0528	0.001	-0.0565	-0.0491	True
DES	Modified AES	-0.0167	0.001	-0.0204	-0.0130	True
Serpent	Modified AES	0.0001	1.000	-0.0037	0.0037	False
Twofish	Modified AES	0.0001	1.000	-0.0037	0.0037	False

Dari tabel 3 di atas, AES modifikasi tidak menunjukkan perbedaan signifikan dibandingkan dengan AES standar, Serpent, dan Twofish dalam hal waktu enkripsi, sedangkan terdapat perbedaan signifikan antara AES modifikasi dan DES serta 3DES, di mana AES modifikasi lebih cepat.

Tabel 4. Hasil Tukey's HSD Test proses dekripsi

Group1	Group2	Meandiff	p-adj	Lower	Upper	reject
AES	Modified AES	-0.0002	0.001	-0.0012	-0.0002	True
3DES	Modified AES	-0.0525	0.001	-0.0535	-0.0515	True
DES	Modified AES	-0.0168	0.001	-0.0178	-0.0158	True
Serpent	Modified AES	0.0002	0.001	0.0002	0.0012	True
Twofish	Modified AES	0.0001	0.001	0.0001	0.0011	True

Dari tabel 4 di atas, AES modifikasi menunjukkan perbedaan signifikan dalam waktu dekripsi dibandingkan dengan AES standar, DES, 3DES, Serpent, dan Twofish dalam waktu dekripsi.

Selanjutnya, kami melakukan eksperimen untuk mengukur *avalanche effect* pada algortima AES termodifikasi, AES, Twofish, DES dan 3DES.

Tabel 5. Hasil Pengujian avalanche effect

Algoritma	Mean Bit Differences	Std Dev Bit Differences
AES	49.63%	4.20%
Modified AES	50.20%	4.23%
Twofish	49.37%	4.35%
Serpent	50.59%	4.29%
DES	51.39%	5.53%
3DES	49.12%	5.97%

Berdasarkan tabel 5, semua algoritma yang diuji menunjukkan *efek avalanche* yang sangat baik, dengan rata-rata perubahan bit lebih dari 49%. Algoritma AES, AES termodifikasi, Twofish, dan Serpent menunjukkan hasil yang konsisten dengan standar deviasi yang relatif rendah. DES dan 3DES juga menunjukkan efek avalanche yang baik, meskipun memiliki standar deviasi yang sedikit lebih tinggi.

Selanjutnya, kami melakukan eksperimen untuk mengukur nilai throughput dari algortima yang kami uji. Kami melakukan pengujian sebanayak 10 kali dengan file yang berbeda.

Tabel 6. Hasil pengujian Througput

Algorithm	Stat	Encryption (Mbps)	Decryption (Mbps)
3DES	Mean	137.31	137.31
	Std Dev	5.4	5.4
	Min	130.26	125.72
	Median	137.74	137.74
	Max	144.55	144.55
AES	Mean	1985.23	2001.88
	Std Dev	184.91	126.58
	Min	1696.25	1690.33
	Median	2038.77	2073.72
	Max	2136.28	2187.16
DES	Mean	335.48	351.9
	Std Dev	30.35	30.35
	Min	285.8	298.32
	Median	355.5	366.58
	Max	410.37	410.37
Modified AES	Mean	1903.43	2015.02
	Std Dev	296.76	126.58
	Min	1280.84	1831.83
	Median	2007.82	2007.82
	Max	2187.16	2187.16
Serpent	Mean	1990.25	2081.25
	Std Dev	344.89	255.62
	Min	1453.35	1591.0
	Median	2077.18	2077.18
	Max	2579.33	2579.33
Twofish	Mean	2000.45	2063.07
	Std Dev	277.49	265.07
	Min	1468.74	1631.79
	Median	2095.56	2095.56
	Max	2414.29	2414.29

Berdasarkan tabel 6, hasil pengujian *throughput* menunjukan bahwa AES dan AES Termodifikasi memiliki throughput yang sangat tinggi untuk enkripsi dan dekripsi. Algoritma Serpent dan *Twofish* juga menunjukkan *throughput* yang tinggi dan konsisten. DES dan 3DES menunjukkan *throughput* yang lebih rendah dibandingkan dengan algoritma yang lainya.

Selanjutnya, kami melakukan analisis ANOVA terhadap nilai throughput tersebut. Hasil menunjukan bahwa nilai F-Statistik untuk enkripsi yaitu 151.60 dan F-Value yaitu 1.68×10^{-30} ,sedangkan untuk deskripsi, nilai F-Statistif dekripsi yaitu 305.66 dan nilai f-value yaitu 2.66×10^{-38}. Hasil ini menunjukkan bahwa terdapat perbedaan yang sangat signifikan dalam throughput enkripsi dan dekripsi antara algoritma yang diuji.

Tabel 7. Hasil Tukey Test Througput Enkripsi

Group 1	Group 2	Mean Difference	p-adj	Lower	Upper	Reject
3DES	AES Termodifikasi	1766.1194	0.0001	1490.60	2041.64	True
AES	AES Termodifikasi	-81.80	0.916	-357.32	193.72	False

DES	AES Termodifikasi	1567.96	0.001	1292.44	1292.44	True
AES Termodifikasi	Serpent	86.82	0.8885	-188.70	362.34	False
AES Termodifikasi	Twofish	97.0255	0.826	-178.50	372.54	False

Tabel 8. Hasil Tukey Test Througput Dekripsi

Group 1	Group 2	Mean ence	p-	Lower	Upper	Rej
3DES	AES Termodifikasi	1878.3536	0.001	1566.11	2101.30	True
AES	AES Termodifikasi	16.5748	0.9999	-205.4736	238.6231	False
DES	AES Termodifikasi	1659.3072	0.0	1437.2589	1881.3555	True
AES Termodifikasi	Serpent	66.2329	0.9494	-155.8154	288.2812	False
AES Termodifikasi	Twofish	48.0541	0.9874	-173.9942	270.1024	False

Hasil uji tukey menunjukan bahwa algoritma AES termodifikasi tidak menunjukkan perbedaan signifikan dengan AES standar, Serpent, dan Twofish dalam throughput enkripsi dan dekripsi, akan tetapi perbedaan signifikan terjadi pada AES Modifikasi dengan DES dan 3DES dalam throughput enkripsi dan dekripsi. Pada proses enkripsi, AES Modifikasi memiliki throughput 467.37% lebih tinggi dibandingkan dengan DES dan 1286.26% lebih tinggi dibandingkan dengan 3DES.

V. KESIMPULAN

Setelah dilakukan analisis kinerja algoritma AES termodifikasi dengan mengganti fungsi Mix Column menjadi bit permutasi dan mengurangi jumlah putaran menjadi 12 terhadap algortima AES konvensional, Serpent, Twofish, 3DES dan DES. Pada pengujian kecepatan AES modifikasi lebih cepat dibanding AES konvensional, Serpent, Twofish, 3DES dan DES. AES termodifikasi memberikan peningkatan kecepatan 0.38% pada proses enkripsi dan 8% pada proses dekripsip dibanding AES Standar . Berdasarkan hasil pengujian, AES termodifikasi menunjukan *Avalanche effect* 50.20% dan AES standar 49.63%. Pengujian throughput menunjukan bahwa tidak terjadi perubahan yang signifikan terhadap algoritma yang diuji pada proses enkripsi, akan tetapi mengalami perbedaan yang signifikan terhadap proses dekripsi. AES modifikasi memiliki *throughput* 467.37% lebih tinggi dibandingkan dengan DES dan 1286.26% lebih tinggi dibandingkan dengan 3DES.

DAFTAR PUSTAKA

[1] U. Arnaut, M. Tair, and M. Veinoviÿ, “Perbandingan efisiensi implementasi aes pada platform web utama,” in *Konferensi Ilmiah Internasional*, Beograd: Singidunum University, 2021, pp. 153–157.

[2] M. A. Al-Shabi, “A Survey on Symmetric and Asymmetric Cryptography Algorithms in information Security,” *International Journal of Scientific and Research Publications (IJSRP)*, vol. 9, no. 3, p. p8779, Mar. 2019, doi: 10.29322/IJSRP.9.03.2019.p8779.

[3] J. S. Baladhay and E. M. De Los Reyes, “AES-128 reduced-round permutation by replacing the MixColumns function,” *Indonesian Journal of Electrical Engineering and Computer Science*, vol. 33, no. 3, pp. 1641–1652, Mar. 2024, doi: 10.11591/ijeecs.v33.i3.pp1641-1652.

[4] H. V. Gamido, “Implementation of a bit permutation-based advanced encryption standard for securing text and image files,” *Indonesian Journal of Electrical Engineering and Computer Science*, vol. 19, no. 3, pp. 1596–1601, Sep. 2020, doi: 10.11591/ijeecs.v19.i3.pp1596-1601.

[5] J. S. Baladhay, H. V. Gamido, and E. M. De Los Reyes, “Large file encryption in a Reduced-Round Permutation-Based AES file management system,” *Indonesian Journal of Electrical Engineering and Computer Science*, vol. 34, no. 3, pp. 2021–2031, Jun. 2024, doi: 10.11591/ijeecs.v34.i3.pp2021-2031.

[6] R. N. Fitriana and D. Djuniadi, “Analisis Perbandingan Algoritma AES Dan RC4 Pada Enkripsi dan Dekripsi Data Teks Berbasis CrypTool 2,” *Systemic: Information System and Informatics Journal*, vol. 7, no. 2, pp. 1–7, Dec. 2022, doi: 10.29080/systemic.v7i2.1263.

[7] “Comparing Symmetric and Asymmetric cryptography in message encryption and decryption by using AES and RSA algorithms,” *JOURNAL OF XI’AN UNIVERSITY OF ARCHITECTURE & TECHNOLOGY*, vol. XII, no. III, Mar. 2020, doi: 10.37896/jxat12.03/262.

[8] O. C. Abikoye, A. D. Haruna, A. Abubakar, N. O. Akande, and E. O. Asani, “Modified Advanced Encryption Standard Algorithm for Information Security,” *Symmetry (Basel)*, vol. 11, no. 12, p. 1484, Dec. 2019, doi: 10.3390/sym11121484.

[9] N. A. Ariffin Mohd and A. Y. Ahmed Ashawesh, “Enhanced AES algorithm based on 14 rounds in securing data and minimizing processing time,” in *Journal of Physics: Conference Series*, IOP Publishing Ltd, Mar. 2021. doi: 10.1088/1742-6596/1793/1/012066.

[10] F. Hazzaa, A. M. Shabut, N. H. M. Ali, and M. Cirstea, “Security Scheme Enhancement for Voice over Wireless Networks,” *Journal of Information Security and Applications*, vol. 58, p. 102798, May 2021, doi: 10.1016/j.jisa.2021.102798.

[11] S. D. Sanap and V. More, “Performance Analysis of Encryption Techniques Based on Avalanche effect and Strict Avalanche Criterion,” in *2021 3rd International Conference on Signal Processing and Communication (ICPSC)*, IEEE, May 2021, pp. 676–679. doi: 10.1109/ICSPC51351.2021.9451784.