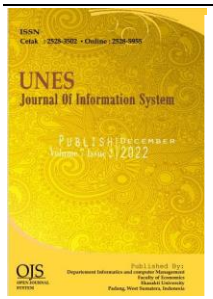

UNES Journal of Information System

Volume 8, Issue 1, June 2023

P-ISSN 2528-3502

E-ISSN 2528-5955

Open Access at: https://fe.ekasakti.org/index.php/UJIS

PERBANDINGAN ALGORITMA KRIPTOGRAFI SIMETRIS DAN ASIMETRIS

COMPARISON OF SYMMETRIC AND ASYMMETRIC CRYPTOGRAPHIC ALGORITHMS

Dedek Indra Gunawan Hts[1)], M. Ridho Aldizar[2)], Irza Fahreza Nasution[3)], Muhammad Farhan Nasution[4)]

[1,2,3,4)]Program Studi Informatika, Fakultas Teknik dan Ilmu Komputer, Universitas Potensi Utama

Email : dedek.indra@gmail.com, aldizar1205@gmail.com, fahrezairza78@gmail.com, nastyfarhan1303@gmail.com

INFO ARTIKEL

Koresponden:

Dedek Indra Gunawan Hutasuhut

dede.indra@gmail.com

Kata kunci

Kriptografi, AES, RSA, Data Siswa

Website:

https://fe.ekasakti.org/index.php/UJIS

Hal: 042 - 047

ABSTRAK

Pada era digital ini kebutuhan akan keamanan di bidang informasi dan teknologi menjadi semakin banyak digunakan dan kerentan dari serangan pihak luar sering dilakukan guna mendapatkan informasi yang berharga, oleh karena itu diperlukan sistem keamanan yang dapat di enkripsi dengan menggunakan algoritma kriptografi yang dapat memberikan jaminan keamanan diantaranya dua algoritma yang digunakan yaitu Advanced Encryption Standard (AES) dan Rivest-Shamir-Adleman (RSA). Penelitian yang dilakukan dengan mempertimbangkan faktor kecepatan dan keamanan dari kedua algoritma. Hasil yang didapatkan dari pengujian tersebut menunjukan algoritma AES lebih unggul dalam hal keamanan dan kecepatan. Dalam hal pengolahan data algoritma AES memberikan kinerja yang sangat baik. Sedangkan algoritma RSA lambat dalam mengolah data. Dapat disimpulkan bahwa algoritma AES memiliki waktu proses eksekusi lebih cepat daripada algoritma RSA.

ARTICLE INFO

Corresponden:
Dedek Indra Gunawan Hutasuhut
dede.indra@gmail.com

Keyword
Cryptography, AES, RSA, Student Data

Website:
https://fe.ekasakti.org/index.php/UJIS

Page: **042 - 047**

ABSTRACT

In this digital era, the need for security in the field of information and technology is becoming increasingly used and the vulnerability of external attacks is often carried out to obtain valuable information, therefore a security system is needed that can be encrypted using cryptographic algorithms that can provide security guarantees, including the two algorithms used are Advanced Encryption Standard (AES) and Rivest-Shamir-Adleman (RSA). The research was conducted by considering the speed and security factors of the two algorithms. The results obtained from these tests show that the AES algorithm is superior in terms of security and speed. In terms of data processing, the AES algorithm provides very good performance. While the RSA algorithm is slow in processing data. It can be concluded that the AES algorithm has a faster execution time than the RSA algorithm.

PENDAHULUAN

Sistem-sistem pada dunia informasi dan teknologi masih banyak yang belum menerapkan keamanan digital seperti kriptografi, dengan perkembangan teknologi yang semakin pesat diiringi juga serangan digital yang rentan dan masif dan didukung internet dengan penyebarannya meluas digunakan untuk berkomunikasi dan mencari informasi, berkomunikasi yang saling mengirim dan menerima informasi menggunakan proses enkripsi dan deskripsi.

Kriptografi adalah teknik untuk memastikan kerahasiaan dan keamanan pesan saat dikirim ke tujuan, mencegah penyadapan. Enkripsi, dekripsi, dan kunci adalah tiga dasar kriptografi. Fungsi utama kriptografi adalah merahasiakan kunci dan mengubah plaintext menjadi ciphertext, sehingga plaintext menjadi password yang tidak diketahui orang lain, tanpa harus merahasiakan algoritma yang digunakan

Kriptografi dapat digolongkan dalam beberapa jenis seperti algoritma hash, algoritma kunci simetris dan algoritma kunci asimetris yang banyak digunakan pada topik penelitian ini golongan kriptografi yang digunakan yaitu kunci simetris dan kunci asimetris.

Algoritma yang masih kuat digunakan hingga saat ini adalah AES dan RSA. AES adalah *Advanced Encryption Standard*. AES telah terbukti menjadi salah satu algoritma yang sangat aman yang digunakan sebagai standar enkripsi untuk informasi rahasia dan digunakan secara luas di seluruh dunia. Hasil yang didapatkan dari algoritma AES berupa data yang terenkripsi secara simetris, sementara dari RSA adalah data yang terenkripsi dengan kunci publik untuk enkripsi dan kunci pribadi untuk deskripsi.

AES merupakan sistem penyandian blok yang bersifat non-Feistel karena AES menggunakan komponen yang selalu memiliki invers dengan panjang blok 128 bit. Kunci AES menggunakan proses yang berulang yang disebut dengan ronde.

Algoritma RSA merupakan salah satu jenis algoritma dalam sistem kriptografi kunci-publik, atau dikenal juga dengan kriptografi asimetris yang adalah bentuk kriptografi dimana pengguna memiliki pasangan kunci kriptografi yaitu kunci publik dan kunci privat

Walaupun begitu setiap algoritma memiliki keunggulan masing-masing sesuai dengan kebutuhan yang berbeda. Algoritma AES yang biasa digunakan untuk enkripsi data berjumlah besar dengan kecepatan tinggi, sedangkan algoritma RSA menggunakan enkripsi kunci simetris yang relatif aman dikarenakan menggunakan kunci.

Menurut penelitian Akhmad Budi yang membahas mengenai "Analisis Perbandingan Algoritma Kriptografi Metode DES dengan Metode AES", didapatkan kesimpulan yaitu kriptografi modern AES lebih aman daripada metode DES karena metode AES memiliki perlindungan ganda.

Menurut penelitian Maya Sari yang membahas mengenai "Algoritma Kriptografi Sistem Keamanan SMS di Android", didapatkan kesimpulan dari penelitian ini dengan membandingkan ketiga algoritma kriptografi yaitu AES, RSA dan TEA dengan cara membandingkan karakteristik algoritma enkripsi dengan menggunakan hasilnya untuk digunakan sebagai sistem keamanan SMS berbasis android mendapatkan hasil dari review yaitu algoritma TEA merupakan algoritma terbaik untuk sistem keamanan SMS di android.

Dalam penulisan ini dilakukan perbandingan antara algoritma AES dan RSA yang membandingkan algoritma simetris dengan algoritma asimetris untuk menentukan algoritma jenis apa yang lebih unggul dalam sisi kecepatan dan keamanannya.

METODE PENELITIAN

Metode yang digunakan pada penelitian kali ini adalah *Studi literatur* yaitu metode yang mengumpulkan semua teori dari penelitian yang telah dilakukan sebelumnya yang berhubungan dengan enkripsi dan deskripsi lalu membandingkannya.

HASIL DAN PEMBAHASAN

Desain Algoritma AES

Proses Enkripsi AES

Proses enkripsi algoritma AES terdiri dari 4 jenis transformasi bytes, yaitu SubBytes, ShiftRows, Mixcolumns dan AddRoundKey. Pada awal proses enkripsi, input yang telah dicopykan ke dalam state akan mengalami transformasi byte AddRoundKey. Setelah itu state akan mengalami transformasi SubBytes, ShiftRows, MixColumns, dan AddRoundKey secara berulang-ulang sebanyak Nr. Proses ini dalam algoritma AES disebut sebagai round function. Round yang terakhir agak berbeda dengan round-round sebelumnya dimana pada round terakhir, state tidak mengalami transformasi MixColumns.

a. SubBytes

   Prinsip dari *SubBytes* adalah menukar isi matriks/tabel yang ada dengan matriks/tabel lain yang disebut dengan Rijndael S-*Box*.

b. ShiftRows

ShiftRows seperti namanya adalah sebuah proses yang melakukan *shift* atau pergeseran pada setiap elemen blok/tabel yang dilakukan per barisnya.

c. Mixcolumns

Yang terjadi saat *MixColumns* adalah mengalikan tiap elemen dari blok chiper dengan matriks dengan pengalian dilakukan seperti perkalian matriks biasa yaitu menggunakan *dot product*.

d. AddRoundKey

AddRoundKey pada dasarnya adalah mengkombinasikan *chiper* teks yang sudah ada dengan *chiper key* yang *chiper key* dengan hubungan XOR.

Proses Dekripsi AES

Transformasi *chiper* dapat dibalikkan dan diimplementasikan ke dalam arah yang berlawan untuk menghasilkan *inverse cipher* yang mudah dipahami untuk algoritma AES. Transformasi *byte* yang digunakan pada *invers chiper* adalah *InvShiftRows, InvSubBytes, InvMixColumns*, dan *AddRoundKey*.

Desain Algoritma RSA

Proses Enkripsi RSA

Berikut ini adalah proses enkripsi dari algoritma RSA

1. Ambil kunci publik penerima pesan *e* dan modulus *n* atau (*e,n*).
2. Pilih plainteks *m* dan ubah isi pesan *m* menjadi pesan dengan nilai ASCII.
3. Potong pesan menjadi blok-blok pesan m_1, m_2, m_3, …. Dengan nilai setiap bloknya adalah $0 \leq m \leq n - 1$.
4. Setiap blok *m* dihitung dengan rumus $c_i = m_i^e$ **mod** *n.*
5. Susun nilai *c* hasil enkripsi dengan susunan c_1, c_2, c_3,….,c_n sehingga diperoleh *chiper* teks dari pesan *m.*

Proses Dekripsi RSA

Dekripsi digunakan untuk mengubah pesan hasil enkripsi (*chipertext)* menjadi pesan asli (*plaintext*) yaitu dengan menggunakan rumus untuk dekripsi RSA sebagai berikut :

P = Cd mod n.

1. Ambil pesan (cipherteks) yang telah diterima.
2. Kemudian ambil kunci rahasia d dan modulus n atau (d,n).
3. Potong pesan menjadi blok-blok pesan c1, c2, c3, ... dengan nilai setiap bloknya adalah $0 \leq c \leq n - 1$.
4. Hitung mi = cid mod n.
5. Susun nilai m hasil dekripsi dengan susunan m1, m2, m3,....,mn sehingga diperoleh plainteks (pesan asli) dari cipherteks yang diterima.

Perbandingan yang dilakukan pada penelitian ini dengan cara mengeksekusi dan menerapkan kedua algoritma kriptografi simetris dan asimteris yaitu AES yang tergolong kedalam simetris dan RSA yang asimetris, perbandingan dilakukan untuk mencari tau waktu eksekusi dan menghitung pendeskripsian waktu dari kedua algoritma.

Pada penelitian ini peneliti menggunakan converter yang dapat menekripsi dan mendeskripsi AES dan RSA. Berikut hasil yang didapatkan dari perolehan waktu eksekusi :

Tabel 1 Perbandingan Waktu *AES* dan *RSA*

No	Plain Text	Jumlah karakter	Waktu *AES*	Waktu *RSA*
1	t	1 karakter	0.8s	0.14s
2	k5	2 karakter	0.4s	0.12s
3	l%2	3 karakter	0.7s	0.9s
4	12ko	4 karakter	0.13s	0.15s
5	admin	5 karakter	0.15s	0.20s

Perbedaan waktu dari kedua algoritma tergolong tidak terlalu jauh, nilai diatas merupakan waktu dari deskripsi dan enkripsi yang di rata-rata kan dengan hitungan per karakter. Hasil menunjukan waktu dari proses eksekusi menunjukana bahwa algoritma AES lebih cepat dibandingkan dengan algoritma RSA.

SIMPULAN

Hasil dari pembahasann di atas kami mengambil kesimpulan bahwa. *AES* digunakan untuk penyandian blok yang bersifat non-Feistel selalu memiliki invers dengan panjang blok 128 bit proses yang berulang yang disebut dengan ronde, sedangkan *RSA* sistem kriptografi kunci-publik dimana pengguna memiliki pasangan kunci kriptografi yaitu kunci publik dan kunci privat.

DAFTAR PUSTAKA

A. Budi, A. Chicali, S. Pengajar, and S. Teknik Informatika, "System (Studi Kasus Pada Pt. One Standard Group Pte Ltd)," *J. Teknol. dan Sist. Komput.*, vol. 3, no. 2, p. 253, 2015.se

M. Sari, H. D. Purnomo, and I. Sembiring, "Review : Algoritma Kriptografi Sistem Keamanan SMS di Android," *J. Inf. Technol.*, vol. 2, no. 1, pp. 11–15, 2022, doi: 10.46229/jifotech.v2i1.292.

A. R. Tulloh *et al.*, "Kriptografi Advanced Encryption Standard (AES) Untuk Penyandian File Dokumen Cryptography Advanced Encryption Standard (AES) for File Document Encryption," *J. Mat. UNISBA*, vol. Vol 2, no. 1, pp. 1–8, 2016.

B. Fachri and R. M. Sembiring, "Pengamanan Data Teks Menggunakan Algoritma DES Berbasis Android," *J. Media Inform. Budidarma*, vol. 4, no. 1, p. 110, 2020, doi: 10.30865/mib.v4i1.1700.

M. Reza and F. Zen, "Algoritma Kriptografi Kunci-publik RSA menggunakan Chinese Remainder Theorem," pp. 1–6.

V. Yuniati, G. Indriyanta, and A. Rachmat C., "Enkripsi Dan Dekripsi Dengan Algoritma Aes 256 Untuk Semua Jenis File," *J. Inform.*, vol. 5, no. 1, 2011, doi: 10.21460/inf.2009.51.69.

D. Nurnaningsih and A. A. Permana, "Rancangan Aplikasi Pengamanan Data Dengan Algoritma Advanced Encyption Standard (Aes)," *J. Tek. Inform.*, vol. 11, no. 2, pp. 177–186, 2018, doi: 10.15408/jti.v11i2.7811.

A. E. Standard *et al.*, "Enkripsi Algoritma AES (Advanced Encryption Standard)," 2001.

F. Muharram, H. Azis, and A. R. Manga, "Analisis Algoritma pada Proses Enkripsi dan Dekripsi File Menggunakan Advanced Encryption Standard (AES)," *Proc. Semin. Nas. Ilmu Komput. dan Teknol. Inf.*, vol. 3, no. 2, pp. 112–115, 2018.

A. P. Wahyadyatmika, R. R. Isnanto, and M. Somantri, "Implementasi Algoritma Kriptografi RSA pada Surat Elektronik (E-Mail)," *Transient*, vol. 3, no. 4, pp. 1–9, 2014.

S. Sulistiyorini and A. Prihanto, "Perbandingan Efisiensi Algoritma RSA dan RSA-CRT Dengan Data Teks Berukuran Besar," *J. Informatics Comput. Sci.*, vol. 1, no. 02, pp. 84–90, 2020, doi: 10.26740/jinacs.v1n02.p84-90.

Weriza, J., Malisza, D., Dahri, N., & Susanti, M. (2021). RESTAURANT MENU DESIGN MUARO NEW SAND JAMAK. Dinasti International Journal of Digital Business Management, 2(6), 1063-1069.

Siregar, J. J. (2013). Analisis explotasi keamanan web denial of service attack. ComTech: Computer, Mathematics and Engineering Applications, 4(2), 1199-1205.

Harry Setya Hadi, Danyl Mallisza, & Hudalinnas. (2023). MOBILE MEDIA CENTER MTQ UNTUK LPTQ SUMATERA BARAT BERBASIS ANDROID. Journal of Scientech Research and Development, 5(1), 420-428. https://doi.org/10.56670/jsrd.v5i1.149