E-ISSN : 2827-9425
P-ISSN : 2828-4666

Aplikasi Enkripsi Dan Dekripsi Data Gambar Menggunakan Algoritma Advanced Encryption Standard

[1]Muh Fajril A. Rabiu, [2]Husdi, [3]Hastuti Dalai
[1]Fakultas Ilmu Komputer,Teknik Informatika, Universitas Ichsan Gorontalo, Gorontalo, Indonesia
Email: [1]Bukhas88@email.com, [2]mr.husdi.unisan.id, [3]hastutidalai@gmail.com

Abstrak - Keamanan data digital menjadi semakin penting dalam era informasi saat ini, termasuk dalam perlindungan data gambar. Penelitian ini bertujuan untuk mengembangkan aplikasi enkripsi dan dekripsi data gambar menggunakan algoritma Advanced Encryption Standard (AES) untuk meningkatkan keamanan data. Untuk lebih memperkuat keamanan kunci pribadi, algoritma RSA digunakan dalam mengamankan kunci pribadi yang digunakan dalam proses enkripsi dan dekripsi. Penerapan algoritma AES pada data gambar menunjukkan bahwa metode ini efektif dalam menjaga kerahasiaan dan integritas data. Hasil penelitian ini menegaskan bahwa algoritma AES dapat diterapkan secara efektif untuk keamanan data gambar. Penggunaan algoritma RSA untuk mengamankan kunci pribadi terbukti memperkuat keamanan, membuatnya lebih sulit bagi kriptanalis untuk mendapatkan kunci pribadi dari algoritma AES yang digunakan. Uji coba aplikasi dilakukan dengan menggunakan metode White Box dan Basis Path yang menghasilkan nilai V(G) = CC = 6, menunjukkan kompleksitas yang dikelola dengan baik. Selain itu, pengujian Black Box menunjukkan kebenaran logika aplikasi, membuktikan bahwa flowchart logika yang digunakan dalam aplikasi adalah benar dan dapat diandalkan. Hasil ini menunjukkan bahwa aplikasi yang dikembangkan dapat dioperasikan dengan efektif dan layak digunakan dalam praktik untuk melindungi data gambar dari ancaman keamanan.

Kata Kunci: enkripsi, dekripsi, keamanan data gambar, algoritma AES, Algoritma RSA.

Abstract - *Digital data security is becoming increasingly important in today's information age, including image data protection. This research aims to develop an image dataencryption and decryption application using the Advanced Encryption Standard (AES) algorithm to improve data security. To further strengthen the security of private keys, the RSA algorithm is used in securing the private keys used in the encryption and decryption process. The application of the AES algorithm on imagedata shows that this method effectively maintains data confidentiality and integrity.The research results confirm that the AES algorithm can be effectively applied for image data security. The RSA algorithm used to secure the private key is performedto strengthen the security, making it more difficult for cryptanalysts to obtain the private key from the AES algorithm used. Application testing is conducted using White-Box and Base Path methods which resulted in a value of V(G) = CC = 6, indicating well-managed complexity. In addition, Black-Box testing shows the correctness of the application logic, proving that the logic flowchart used in the application is correct and reliable. It means that the application developed can beoperated effectively and, in practice, is feasible to protect image data from securitythreats.*

Keywords: *encryption, decryption, image data security, AES algorithm, RSA Algorithm.*

1. PENDAHULUAN

Dalam era digital yang semakin maju ini, keamanan data telah menjadi isu yang sangat penting. Dalam lingkungan yang terhubung secara digital, data yang disimpan dan ditransmisikan rentan terhadap ancaman dan serangan yang dapat mengakibatkan kerugian signifikan [1], seperti kerugian finansial dan privasi. Agar keamanannya terjaga maka ilmu yang dikembangkan untuk menjaga keamanan data tersebut adalah kriptografi. Kriptografi adalah suatu ilmu yang mempelajari bagaimana cara menjaga agar data atau pesan tetap aman saat dikirimkan, dari pengirim ke penerima tanpa mengalami gangguan dari pihak ketiga [2].

Berdasarkan jenis kunci yang digunakan, kriptografi terbagi atas dua metode, yaitu kriptografi kunci simetris dan kriptografi kunci asimetris. Perbedaan dari kedua kriptografi ini terletak pada penggunaan kunci [3]. Untuk kriptografi simetris menggunakan kunci yang sama pada saat

E-ISSN : 2827-9425
P-ISSN : 2828-4666

melakukan enkripsi dan dekripsi, salah satu algoritma simetris yaitu AES (Advanced Encryption Satndard) [4]. Oleh sebab itu harus benar-benar dijaga kerahasian kunci tersebut, namun berbeda halnya dengan kriptografi asimetris, kunci pada saat enkripsi berbeda dengan kunci yang digunakan pada saat melakukan dekripsi, hal ini menjadi salah satu faktor kriptografi asimetris lebih aman dibandingkan dengan kriptografi simetris [5], salah satu algoritma asimetris yaitu RSA.

AES digunakan sebagai standar algoritma kriptografi terbaru yang dipublikasikan oleh NIST (National Institute of Standard and Technology) sebagai pengganti algoritma DES (Data Encryption Standard) yang sudah berakhir masa penggunaannya [6]. Algoritma AES adalah algoritma kriptografi yang dapat mengenkripsi dan mendekripsi data dengan panjang kunci yang bervariasi, yaitu 128 bit, 192 bit, dan 256 bit [4]. Sedangkan Algoritma asimetris yang paling populer adalah RSA. Algoritma RSA dibuat oleh 3 orang peneliti dari MIT (*Massachussets institute of Technology*) pada tahun 1976, yaitu Rivets, Shamir, dan Adleman. Algoritma ini menggunakan pemfaktoran bilangan yang sangat besar, Oleh karena alasan tersebut RSA dianggap aman [7].

Pada penelitian yang dilakukan oleh Faturungi Muharram, Huzain Azis, dan Abdul Rachman Manga dengan judul **"**Analisis Algoritma pada Proses Enkripsi dan Dekripsi File Menggunakan Advanced Encryption Standard (AES**)"**, dengan tujuan mengamankan data gambar menggunakan algoritma AES. Dari penelitian ini gambar berhasil dienkripsi dan dikembalikan ke bentuk aslinya, waktu yang dibutuhkan saat enkripsi dan dekripsi dipengaruhi oleh besarnya ukuran data. Penelitian yang dilakukan oleh Steven Richardo Siburian [8], tentang kombinasi AES dan RSA untuk enkripsi teks pesan, pada penelitian ini di buat sebuah program python untuk mengimplementasikan kombinasi AES dan RSA untuk enkripsi teks. Selanjutnya penelitian yang dilakukan oleh Muhamad Andra Fahreza dan Arif Harbani dengan judul Aplikasi Keamanan Data Gambar Menggunakan Algoritma RSA (Rivest Shamir Adleman) Berbasis Desktop. Algortima RSA digunakan untuk mengamankan file gambar.

Algoritma AES memiliki kelemahan Dari segi jenis kunci yang simetris dimana pengirim dan penerima data memiliki kunci yang sama untuk setiap proses pengiriman-penerimaan data, hal ini akan menyebabkan kunci mudah bocor meskipun dalam waktu yang lama [9]. Untuk meningkatkan keamanan dalam proses enkripsi dan dekripsi data gambar maka dilakukan kombinasi algortima simetris (AES) dan asimetris (RSA). AES di gunakan untuk mengenkripsi data atau gambar dengan kunci simetris yang cepat dan efisien, sedangkan pada RSA di gunakan untuk mengenkripsi kunci simetris tersebut dengan kunci public penerima. Dengan kombinasi ini gambar dapat diamankan dengan enkripsi yang kuat saat pengiriman dan hanya pemegang kunci privat yang dapat mengakses dan mendekripsi gambar tersebut [8]. Dengan kombinasi algortima AES dan RSA, suatu informasi akan menjadi lebih sulit untuk diketahui oleh orang yang tidak berhak. Kemanan tersebut di perlukan untuk menghindari adanya penyadapan atau pembajakan gambar yang mengandung informasi penting bagi penggunanya. Keamanan diperlukan untuk menjaga integritas gambar tersebut agar tetap aman [7].

2. TINJAUAN PUSTAKA

2.1 Algoritma Advanced Encyrption Standard

Algoritma AES merupakan algoritma simetris yaitu mengunakan kunci yang sama untuk proses enkripsi dan dekripsi. Algoritma AES memiliki tiga pilihan kunci yaitu tipe: AES-128, AES-192 dan AES-256 [7]. *Advanced Encryption Standard* (AES) dipublikasikan oleh NIST (*National Institute of Standard and Tchnology*) pada tahun 2001. AES merupakan blok kode simetris untuk mengantikan DES (*Data Encryption Standard*) [4]. AES adalah algoritma kriptografi yang dapat mengenkripsi dan mendekripsi data dengan panjang kunci yang bervariasi, yaitu 128 bit, 192 bit, dan 256 bit [7]. Perbedaan panjang kunci ini yang nantinya mempengaruhi jumlah putaran pada algoritma AES ini. Jumlah putaran yang digunakan algoritma ini ada tiga macam seperti pada Tabel 2.1.

Tabel 1. Parameter AES [4].

Algoritma	Jumlah Key (Nk)	Ukuran Block (Nb)	Jumlah Putaran (Nr)
AES-128	4	4	10

E-ISSN : 2827-9425
P-ISSN : 2828-4666

AES-192	6	4	12
AES-256	8	4	14

2.1.1 Prosese Enkripsi dan Dekripsi AES

Proses enkripsi algoritma AES terdiri dari 4 jenis transformasi bytes, yaitu SubBytes, ShiftRows, Mixcolumns dan AddRoundKey , sedangkan proses dekripsi yaitu invShiftRows, InvMixColumns, dan AddRoundKey [7].

2.2 Algoritma RSA

Algoritma RSA dibuat oleh Ron Rivest, Adi Shamir, dan Leonard Adleman, tiga orang peneliti dari MIT (*Massachussets Institute of Technology*) pada tahun 1976. RSA termasuk ke dalam skema kriptografi asimetris. Kriptografi asimetris merupakan algoritma kriptografi yang menggunakan kunci yang berbeda yaitu kunci publik (*public key*) dan kunci rahasia (*private key*) pada proses enkripsi dan dekripsinya. Kunci publik dapat mengenkripsi pesan namun tidak dapat mendekripsi pesan [10].

Tabel 2. Properti algoritma RSA [10]**.**

Properti	Properti Algoritma	Kerahasiaan
p	bilangan prima	rahasia
q	bilangan prima	rahasia
n	$n = p \times q$	tidak rahasia
ϕ	$\phi(n) = (p - 1)(q - 1)$	rahasia
e	Kunci enkripsi, yang memenuhi $FPB(e, \phi(n)) = 1$	tidak rahasia

Pada tahap pembangkitan kunci, dilakukan beberapa langkah sebagai berikut.

1. Pilih dua bilangan prima p dan q.
2. Hitung
   $n = p \times q$ (1)
   ($p \neq q$ agar n tidak mudah difaktorkan)
3. Hitung
   $\phi(n) = (p - 1)(q - 1)$ (2)
4. Pilih kunci publik e, yang relatif prima terhadap $\phi(n)$.
5. Bangkitkan d yang memenuhi
   $e.d = 1 \ mod \ \phi(n)$ (3)

Kemudian, proses enkripsinya adalah sebagai berikut.

1. Ambil kunci publik penerima pesan , dan modulus .
2. Nyatakan *plainteks* m menjadi blok-blok m_1 , m_2 , …, sedemikian sehingga setiap blok merepresentasikan nilai di dalam selang [0,n - 1] .
3. Setiap blok m_i dienkripsi menjadi blok c_i dengan rumus
   $c_i = m_i^e \ mod \ n$ (4)

Pada proses dekripsi, setiap blok *cipherteks* didekripsi kembali menjadi blok mi dengan rumus $m_i = c_i^d \ mod \ n$ [10].

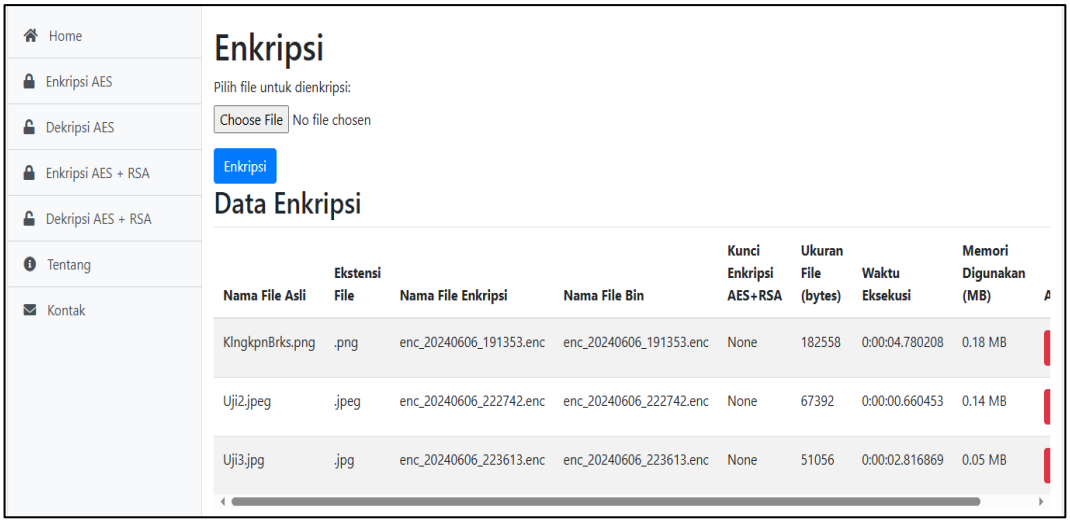
3. METODE PENELITIAN

Penelitian ini menggunakan metode *eksperimen*. Dengan demikian jenis penelitian ini adalah penelitian *eksperimental*. Pengumpulan data yang dikumpulkan menggunakan *Studi Literatur*. Dengan mengumpulkan barbagai macam referensi seperti jurnal terkait dari internet yang berhubungan dengan kombinasi algoritma AES dan RSA untuk enkripsi dan dekripsi data gambar.

E-ISSN : 2827-9425
P-ISSN : 2828-4666

4. HASIL DAN PEMBAHASAN

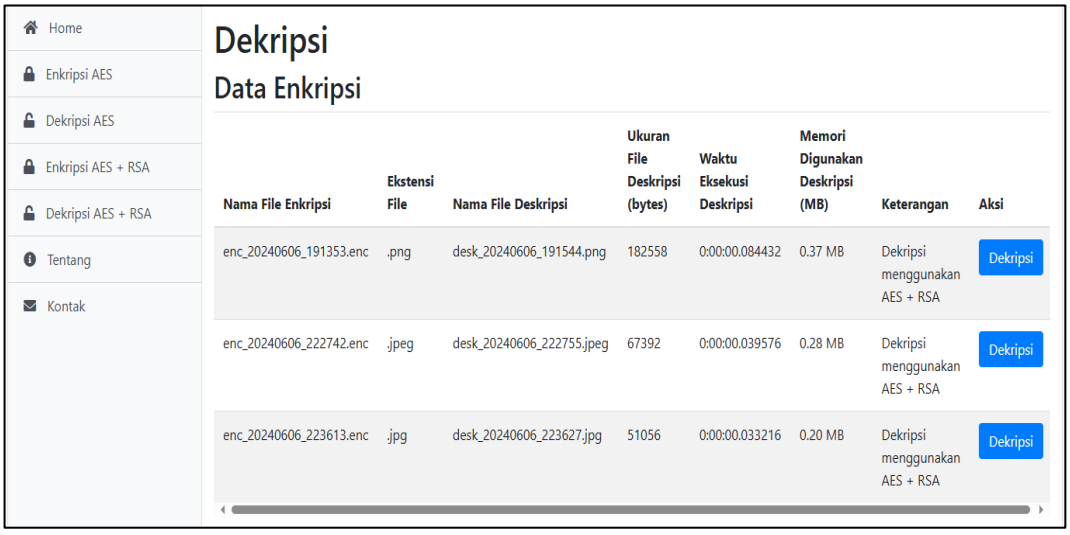
4.4 Tampilan Menu Enkripsi AES dan RSA



Gambar 1. Tampilan Menu Enkripsi AES dan RSA

Pada menu ini dilakukan enkripsi gambar menggunakan algortima AES kemudian kunci AES di enkripsi menggunakan algortima RSA.

4.2 Tampilan Menu Dekripsi AES dan RSA



Gambar 2. Tampilan Menu Dekripsi AES dan RSA

Pada menu ini dilakukan dekripsi kunci AES menggunakan algortima RSA kemudian barulah gambar hasil enkripsi di dekrpisi menggunakan Algortima AES.

E-ISSN : 2827-9425
P-ISSN : 2828-4666

4.3 Hasil Uji Coba

1. Enkripsi AES dan RSA

Tabel 3. Kinerja Enkripsi AES dan RSA

Nama File	Ukuran File	Waktu Enkripsi	File Hasil Enkripsi	Ukuran File(byte)
KlngkpnBrks.png	178kb	4 s	enc_20240606_191353.enc	182kb
Uji2.jpeg	65kb	66 ms	enc_20240606_222742.enc	67kb
Uji3.jpg	49kb	2 s	enc_20240606_223613.enc	51kb

2. Dekripsi AES dan RSA

Tabel 4. Kinerja Dekripsi AES dan RSA

Nama File	Ukuran File(byte)	Waktu Enkripsi	File Hasil Dekripsi
enc_20240606_191353.enc	182kb	8 ms	desk_20240606_191544.png
enc_20240606_222742.enc	67kb	3 ms	desk_20240606_222755.jpeg
enc_20240606_223613.enc	51kb	3 ms	desk_20240606_223627.jpg

Berdasarkan kinerja enkripsi dan dekripsi dapat disimpulkan bahwa sistem dapat melakukan proses enkripsi dan dekripsi gambar mengggunakan algoritma AES dan melakukan enkripsi dan dekripsi kunci pribadi menggunakan algoritma RSA.

5. KESIMPULAN

Algoritma AES dapat diterapkan untuk keamanan data gambar. algortima RSA yang digunakan untuk mengamankan kunci pribadi dapat memperkuat keamanan kunci pribadi sehingga kriptanalis lebih sulit untuk mendapatkan kunci pribadi dari algoritma AES yang digunakan untuk mengenkripsi dan dekripsi data gambar.

DAFTAR PUSTAKA

[1] A. Pratama, M. N. Arif, M. Nazir, and Z. Dannaun, "Algoritma Des (Data Encryption Standard) Untuk," *J. Siteba*, vol. 2, no. 1, pp. 15–18, 2023.

[2] Azlin, F. Musadat, and J. Nur, "Aplikasi Kriptografi Keamanan Data Menggunakan Algoritma Base64," *J. Inform.*, vol. 7, no. 2, pp. 1–5, 2018.

[3] T. Limbong, U. Katolik, S. Thomas, and S. Utara, "Pengujian kriptografi klasik caesar

E-ISSN : 2827-9425
P-ISSN : 2828-4666

chipper menggunakan matlab," no. September 2015, 2017.

[4] D. Ariyus, *Pengantar Ilmu Kriptografi Teori, Analisis dan Implementasi.* Yogyakarta: Penerit Andi, 2008.

[5] N. E. Saragih, D. Universitas, and P. Utama, "Implementasi Algoritma One Time Pad," no. 3, pp. 31–40, 1924.

[6] S. H. Putra, E. Santoso, and L. Muflikhah, "Implementasi Algoritma Kriptografi Advanced Encryption Standard (AES) Pada Kompresi Data Teks," *J. Ilmu Komput.*, pp. 1–14, 2013.

[7] 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.

[8] S. R. Siburian, R. Alek, S. Sinaga, and F. Yudistira, "Kriptosistem Hybrid Menggunakan Kombinasi Aes Dan Rsa Untuk Enkripsi Teks Pesan," *J. JOCOTIS - J. Sci. Inform. Robot.*, vol. 1, no. 1, pp. 22–31, 2023, [Online]. Available: https://jurnal.ittc.web.id/index.php/jct/

[9] Asriyanik, "Studi Terhadap Advanced Encryption Standard (Aes) Dan," *J. Ilm. Sains dan Teknol.*, vol. 7, no. 1, pp. 553–561, 2017.

[10] P. E-mail, "Program Studi Matematika, FPMIPA, Universitas Pendidikan Indonesia e-mail:," vol. 3, no. 2, pp. 92–101, 2023.