ANALISIS TEKNIK ENKRIPSI DALAM KEAMANAN DATA DIGITAL

Maria Emiliana Naipoen[1], Stefani Ribyka Sasi[2], Maria Rosilinda Lahini[3], Maria Lidiana Hoar Suri[4], Siprianus Septian Manek[5]
naipoenmilan@gmail.com[1], sasiribyka@gmail.com[2], rosilindalahini@gmail.com[3], lidiasury67@gmail.com[4], epimanek18@gmail.com[5]
Universitas Timor

ABSTRAK

Keamanan data digital menjadi aspek krusial dalam era informasi yang semakin berkembang. Teknik enkripsi digunakan untuk melindungi data dari akses tidak sah dengan mengubahnya menjadi format yang tidak dapat dibaca tanpa kunci dekripsi. Penelitian ini menganalisis berbagai teknik enkripsi yang digunakan dalam keamanan data digital, mencakup algoritma simetris dan asimetris, serta efektivitasnya dalam melindungi informasi. Studi ini juga mencakup simulasi dan perhitungan algoritma enkripsi untuk mengevaluasi kinerja dan tingkat keamanan masing-masing metode. Hasil analisis menunjukkan bahwa pemilihan algoritma enkripsi yang tepat bergantung pada faktor seperti kecepatan, kompleksitas, dan kebutuhan keamanan data. Temuan ini diharapkan dapat memberikan wawasan bagi pengembang sistem keamanan dalam memilih teknik enkripsi yang optimal sesuai dengan kebutuhan.

Kata Kunci: Enkripsi, Keamanan Data, Algoritma Simetris, Algoritma Asimetris, Keamanan Informasi.

ABSTRACT

Digital data security is a crusial aspect in the rapidly evolving information era. Encryption techniques are used to protect data from unauthorized access by transforming it into an unreadable format without a descryption key. This study analyzes various encryption algorithms and their effectiveness in safeguarding information. The research also includes simulations and encryption algorithm calculations to evaluate the performance and security levels of each method. The analisys results indicate the selecting the appropriate encryption algorithm depends on factors such as speed, complexity, and data security requirements. These findings are expected to provide insight for security system developers in choosing the most suitable encryption techniques based on specific needs.

Keywords: *Encryption, Data Security, Symmetric Algorithm, Asymmetric Algorithm, Information Security.*

PENDAHULUAN

Dalam era digital yang semakin berkembang Keamanan data telah menjadi salah satu masalah paling penting yang dihadapi oleh banyak negara, termasuk Indonesia, dalam era digital yang semakin maju.

Peningkatan penggunaan teknologi informasi dalam berbagai sektor, seperti perbankan, kesehatan, pemerintahan, dan komunikasi, menyebabkan meningkatnya ancaman terhadap data digital, termasuk peretasan, pencurian data, dan akses tidak sah. Oleh karena itu, perlindungan data melalui teknik enkripsi menjadi suatu keharusan untuk memastikan keamanan dan integritas informasi.

Enkripsi merupakan proses mengubah data menjadi format yang tidak dapat dibaca tanpa kunci dekripsi yang sesuai. Teknik ini bertujuan untuk melindungi informasi dari akses tidak sah, baik dalam penyimpanan maupun dalam proses transmisi. Terdapat berbagai algoritma enkripsi yang dikembangkan untuk meningkatkan keamanan data, termasuk algoritma simetris seperti AES (Advanced Encryption Standard) dan DES (Data Encryption Standard), serta algoritma asimetris seperti RSA (Rivest-Shamir-Adleman) dan

ECC (Elliptic Curve Cryptography). Setiap algoritma memiliki kelebihan dan kekurangan dalam hal kecepatan, kompleksitas, serta tingkat keamanan yang ditawarkan. Pendidikan memiliki peran penting dalam membentuk karakter individu agar mampu menggunakan teknologi informasi secara bijak dan bertanggung jawab. Dengan pendidikan, individu dapat memahami nilai-nilai etika, seperti kejujuran, tanggung jawab, dan kepedulian sosial, yang dapat diterapkan dalam penggunaan teknologi. Integrasi pendidikan etika dalam kurikulum pendidikan formal maupun non-formal diharapkan dapat menciptakan generasi yang tidak hanya cerdas secara teknologi, tetapi juga memiliki kesadaran moral yang tinggi.

Penelitian ini bertujuan untuk menganalisis berbagai teknik enkripsi yang digunakan dalam keamanan data digital, baik dari sisi teori maupun melalui simulasi dan perhitungan algoritma. Dengan memahami keunggulan dan kelemahan dari setiap metode enkripsi, diharapkan penelitian ini dapat memberikan wawasan yang lebih dalam bagi pengembang sistem keamanan dalam memilih teknik enkripsi yang optimal sesuai dengan kebutuhan spesifik.

METODE PENELITIAN

Metodologi penelitian ini menggunakan pendekatan deskriptif dan eksperimental untuk menganalisis efektivitas teknik enkripsi dalam keamanan data digital. Data diperoleh melalui kajian literatur dan simulasi algoritma enkripsi seperti AES, DES, RSA, dan ECC menggunakan perangkat lunak Python atau MATLAB. Penelitian ini mengumpulkan data primer dari hasil simulasi dan data sekunder dari sumber ilmiah terkait. Analisis dilakukan secara sistematis melalui identifikasi, implementasi, dan evaluasi algoritma berdasarkan parameter kecepatan, kompleksitas komputasi, dan tingkat keamanan. Hasil simulasi kemudian dianalisis secara komparatif untuk menentukan algoritma yang paling efisien dan aman dalam konteks perlindungan data digital.

HASIL DAN PEMBAHASAN

Pembahasan dilakukan berdasarkan parameter utama, yaitu kecepatan enkripsi/dekripsi, kompleksitas komputasi, dan tingkat keamanan.

1. Hasil Simulasi Algoritma Enkripsi

Simulasi dilakukan terhadap beberapa algoritma enkripsi populer, yaitu AES (Advanced Encryption Standard), DES (Data Encryption Standard), RSA (Rivest-Shamir-Adleman), dan ECC (Elliptic Curve Cryptography). Berikut adalah hasil yang diperoleh dari pengujian algoritma enkripsi berdasarkan ukuran data yang berbeda:

Algoritma	**Waktu Enkripsi (ms)**	**Waktu Deskripsi (ms)**	**Keamanan**
AES (256-bit)	Cepat (~2-5 ms)	Cepat (~3-6 ms)	Sangat Tinggi
DES	Lambat (~10-20 ms)	Lambat (~12-22 ms)	Rendah (Tergolong usang)
RSA (2048-bit)	Sangat Lambat (~50-100 ms)	Sangat Lambat (~60-120 ms)	Sangat tinggi

ECC (256-bit)	Cepat (~5-10 ms)	Cepat (~6-12 ms)	Sangat tinngi

2. Analisis Performa dan Efisiensi

Dari hasil simulasi, dapat disimpulkan beberapa hal berikut:

- AES memiliki kecepatan terbaik untuk enkripsi dan dekripsi, menjadikannya pilihan utama dalam sistem keamanan data digital.
- DES menunjukkan performa yang lebih lambat dan tingkat keamanan yang lebih rendah, sehingga kurang direkomendasikan untuk sistem modern.
- RSA memiliki tingkat keamanan tinggi, tetapi proses enkripsi dan dekripsi lebih lambat, menjadikannya lebih cocok untuk sistem yang membutuhkan autentikasi dan enkripsi data dalam skala kecil.
- ECC memberikan keamanan tinggi dengan efisiensi yang lebih baik dibandingkan RSA, sehingga sering digunakan dalam aplikasi yang memerlukan keamanan tinggi tetapi tetap efisien dalam pemrosesan.

3. Evaluasi Keamanan Algoritma

Keamanan algoritma ditentukan oleh kompleksitas matematisnya dan ketahanannya terhadap serangan kriptografi. Berdasarkan analisis ini:

- AES dan ECC sangat direkomendasikan karena memiliki keseimbangan antara kecepatan dan keamanan.
- RSA tetap menjadi pilihan kuat untuk kriptografi berbasis kunci publik, tetapi dengan kebutuhan komputasi yang lebih besar.
- DES tidak lagi aman karena rentan terhadap serangan brute-force dan sudah ditinggalkan dalam banyak implementasi modern.

4. Implikasi dan Rekomendasi

Berdasarkan hasil penelitian, pemilihan algoritma enkripsi bergantung pada kebutuhan spesifik:

- Untuk keamanan data besar dengan kecepatan tinggi, AES adalah pilihan terbaik.
- Untuk keamanan komunikasi dan tanda tangan digital, ECC lebih efisien dibandingkan RSA.
- Untuk aplikasi yang masih menggunakan DES, sebaiknya segera beralih ke AES atau algoritma modern lainnya untuk meningkatkan keamanan.

KESIMPULAN

Berdasarkan hasil penelitian dan analisis terhadap berbagai teknik enkripsi dalam keamanan data digital, dapat disimpulkan beberapa poin utama sebagai berikut:

1. Enkripsi merupakan aspek penting dalam keamanan data digital, yang berfungsi untuk melindungi informasi dari akses tidak sah dengan mengubahnya menjadi format yang tidak dapat dibaca tanpa kunci dekripsi.
2. Terdapat dua kategori utama algoritma enkripsi, yaitu simetris (menggunakan satu kunci untuk enkripsi dan dekripsi, seperti AES dan DES) serta asimetris (menggunakan dua kunci berbeda, seperti RSA dan ECC).
3. Hasil simulasi menunjukkan bahwa AES memiliki kinerja terbaik dalam hal kecepatan dan keamanan, menjadikannya pilihan utama dalam banyak sistem keamanan modern. Sementara itu, ECC menawarkan keamanan tinggi dengan efisiensi komputasi yang lebih baik dibandingkan RSA.
4. Algoritma RSA tetap menjadi standar dalam kriptografi berbasis kunci publik, meskipun memiliki waktu pemrosesan yang lebih lama dibandingkan ECC. Oleh karena itu, ECC lebih disarankan untuk sistem yang membutuhkan keseimbangan antara keamanan dan

efisiensi.

5. DES terbukti tidak lagi aman untuk digunakan, karena rentan terhadap serangan brute-force dan memiliki kecepatan yang lebih lambat dibandingkan algoritma modern seperti AES.
6. Pemilihan algoritma enkripsi harus disesuaikan dengan kebutuhan spesifik sistem, dengan mempertimbangkan faktor-faktor seperti kecepatan, tingkat keamanan, dan kompleksitas komputasi.

DAFTAR PUSTAKA

R. Al Ihsan and B. A. Sekti, “Pentingnya Keamanan Data Dalam Era Digital : Refleksi Terhadap Serangan Hacker Pada Pusat Data Nasional Indonesia,” pp. 2–6, 2023.