IMPLEMENTASI DAN ANALISIS KEAMANAN ALGORITMA ENKRIPSI PADA SISTEM INFORMASI MODERN

Apriyanti Waltrudis Nino[1], Cantika Natasya Magdalena Kelendonu[2], Sephia Dwi Maryana Ang[3], Kristina Valeriana Ponis[4], Siprianus Septian Manek[5]
apriyantiwltrds@gmail.com[1], ckelendonu@gmail.com[2], sephiaang@gmail.com[3], kristinaponis@gmail.com[4], epimanek18@gmail.com[5]
Universitas Timor

ABSTRAK

Dalam era digital saat ini, keamanan informasi menjadi aspek krusial dalam pengelolaan sistem informasi modern. Ancaman terhadap data seperti pencurian, penyadapan, dan peretasan semakin meningkat seiring dengan pesatnya perkembangan teknologi. Enkripsi merupakan salah satu metode utama yang digunakan untuk menjaga kerahasiaan, integritas, dan keamanan data. Penelitian ini bertujuan untuk mengkaji implementasi algoritma enkripsi dalam sistem informasi modern serta menganalisis tingkat keamanan dari beberapa algoritma populer, baik yang bersifat simetris maupun asimetris. Metodologi yang digunakan mencakup studi literatur dan analisis komparatif terhadap algoritma seperti AES, RSA, dan lainnya. Hasil analisis menunjukkan bahwa pemilihan algoritma enkripsi harus disesuaikan dengan kebutuhan sistem, jenis data, dan tingkat ancaman yang dihadapi. Dengan implementasi yang tepat, algoritma enkripsi dapat secara signifikan meningkatkan perlindungan data pada sistem informasi modern.

Kata Kunci: Keamanan Informasi, Enkripsi, Algoritma Simetris, Algoritma Asimetris, SI Modern.

PENDAHULUAN

Dalam era digital yang serba cepat ini, kita semua tahu bahwa teknologi informasi telah membawa perubahan besar dalam berbagai aspek kehidupan. Namun, di balik kemudahan dan kecepatan yang ditawarkan, ada ancaman serius terhadap keamanan data kita. Sistem informasi modern yang semakin kompleks dan terhubung secara global telah meningkatkan risiko pencurian, peretasan dan manipulasi data. Oleh karena itu, kita perlu mencari solusi efektif untuk melindungi data dan informasi kita dari serangan-serangan tersebut.

Dalam konteks ini, algoritma enkripsi menjadi sangat penting. Namun, pertanyaan yang muncul adalah bagaimana algoritma enkripsi dapat meningkatkan keamanan data pada sistem informasi modern dan algoritma enkripsi apa yang paling efektif digunakan dalam sistem informasi modern.

Artikel ini bertujuan untuk menjelaskan penerapan algoritma enkripsi dalam sistem informasi modern dan menganalisis tingkat keamanan beberapa algoritma enkripsi data dan bagaimana mengimplementasikannya dengan efektif.

METODE PENELITIAN

Jenis Penelitian

Penelitian ini menggunakan pendekatan studi literatur dengan analisis kualitatif guna mengevaluasi penerapan enkripsi dalam sistem informasi. Fokus utama penelitian ini adalah untuk mengkaji serta membandingkan keunggulan dan keterbatasan dari algoritma kriptografi simetris dan asimetris. Tujuannya adalah untuk memberikan pemahaman yang lebih dalam mengenai kontribusi masing-masing jenis kriptografi dalam meningkatkan keamanan data.

HASIL DAN PEMBAHASAN

1. Implementasi Enkripsi pada Sistem Informasi

a. Penerapan AES-128 untuk Keamanan Data Pasien (Berdasarkan Jurnal dari Polinema)
   1) Jurnal 1: Perbandingan Kriptografi Simetris dan Asimetris
      Algoritma kriptografi simetris seperti AES dan RC-5 digunakan dalam sistem informasi untuk mengenkripsi data yang dikirim maupun disimpan. Enkripsi dan deskripsi dilakukan mengguanakan satu kunci yang sama, sehingga prosesnya berlangsung cepat dan efisien. Penggunaan metode ini membantu menjaga kerahasiaan informasi, khususnya dalam komunikasi dan penyimpanan data penting.
   2) Jurnal 2: Penggunaan AES-128 untuk Keamanan Database
      Dalam sistem pendaftaran pasien, data penting seperti NIK, nama, dan alamat diamankan menggunakan algoritma AES-128 sebelum disimpan ke dalam baris data. Langkah ini bertujuan untuk mencegah akses dari pihak yang tidak berwenang dan menjaga kerahasiaan informasi pasien. Hanya pihak yang memiliki kunci enkripsi yang benar yang dapat mendeskripsi dan membaca data tersebut.
   3) Jurnal 3: Pendekatan Kriptografi Hibrid
      Jurnal ini menggabungkan kriptografi simetris dan asimetris demi peningkatan keamanan data. Data utama dienkripsi menggunakan algoritma simetris seperti RC-5 untuk efisiensi, sementara kunci simetrisnya diamankan dengan metode kriptografi asimetris. Dengan menggunakan kunci publik untuk mengenkripsi kunci simetris dan kunci privat untuk deskripsinya, hanya penerima sah yang dapat mengakses data asli.

b. Penggunaan RSA untuk Pertukaran Kunci dalam Sistem Berbasis Cloud
   1) Jurnal 1: Integrasi Kriptografi Simetris dan Asimetris
      Sistem informasi ini menggabungkan penggunaan algoritma kriptografi simetris dan asimetris untuk menjaga keamanan data. Misalnya, data penting dienkripsi menggunakan algoritma simetris seperti AES untuk mendapatkan efisiensi dalam pemrosesan. Selanjutnya, kunnci enkripsi tersebut diamankan dengan metode asimetris, sehingga hanya pihak yang memiliki kunci privat yang dapat mengakses data terenkripsi.
   2) Jurnal 2: Penerapan AES-128 pada Sistem Pendaftaran Pasien
      Pada sistem registrasi pasien, algoritma AES-128 digunakan untuk mengenkripsi data pribadi seperti NIK, nama, dan alamat. Enkripsi dilakukan saat data dimasukan oleh pengguna sebelum disimpan ke database, memastikan bahwa data tidak dapat diakses oleh pihak yang tidak memiliki izin. Antarmuka aplikasi dirancang agar petugas kesehatan dapat melakukan enkripsi dan deskrpsi dengan mudah, tanpa memerlukan pemahaman teknis yang kompleks.
   3) Jurnal 3: Metode Kriptografi Hibrid
      Aplikasi ini menggunakan kombinasi kriptografi simetris dan asimetris guna menciptakan perlindungan data yang lebih kuat. Informasi pengguna dienkripsi menggunakan algoritma simetris seperti RC-5 untuk kecepatan proses, dan kunci simetris tersebut dikirim secara aman menggunakan enkripsi kunci publik. Hanya penerima dengan kunci privat yang dapat mendeskripsinya. Sistem juga menyediakan fitur registrasi dan login, dimana setiap sesi pengguna memiliki kunci sesi tersendiri untuk meningkatkan keamanan selama pertukaran data.

Integrasi dalam Aplikasi Kecepatan Proses Enkripsi dan Deskripsi

a. Jurnal 1: Perbandingan Kriptografi Simetris dan Asimetris
   Algoritma kriptogarfi simetris seperti RC-5 dan AES memilliki keunggulan dalam hal

kecepatan, baik saat melakukan enkripsi maupun deskripsi. Proses ini hanya memerlukan waktu dalam hitungan milidetik, menjadikannya sangat cocok untuk aplikasi yang membutuhkan pemrosesan data secara instan.

b. Jurnal 2: Implementasi AES-128
Hasil pengujian menunjukan bahwa algoritma AES-128 mampu mengenkripsi data dengan sangat cepat. Hal ini menjadikannya pilihan ideal dalam sistem registrasi pasien, di mana waktu respons yang cepat sangat penting untuk akses data yang efisien.

c. Jurnal 3: Pendekatan Hibrid
Dengan memadukan enkripsi simetris untuk efisiensi dan enkripsi asimetris untuk pengelolaan kunci, sistem ini mampu mempertahankan kecepatan pemrosesan tinggi sekkaligus menjaga tingkat keamanan yang optimal.

Tingkat Keamanan

a. Jurnal 1: Analisis Kekuatan Keamanan
Algoritma simetris seperti AES dan RC-5 memiliki panjang kunci yang cukup besar (128 bit ataiuu lebih), yang membuatnya tahan terhadap serangan brute force karena jumlah kombinasi yang harus diuji sangat banyak. Di sisi lain, kriptografi asimetris lebih unggul dalam melindungi data dari serangan man-in-the-middle karena distribusi kunci publik tidak mengungkapkan kunci privat.

b. Jurnal 2: Keamanan AES-128
AES terbukti memiliki tingkat keamanan yang tinnggi melalui berbagai pengujian. Panjang kuncinya membuat upaya brute force menjadi sangat tidak efektif, sehingga data tetap aman dari akses tidak sah.

c. Jurnal 3: Pendekatan Hibrid
Pendekatan gabuangan antara kriptografi simetris dan asimetris meningkatkan proteksi secara menyeluruh. Kunci simetris yang digunakan untuk mengenkripsi data dilindunngi oleh kriptografi asimetris, khususnya melalui kunci publik, yang mencegah risiko serangan selama proses pengiriman data. Selain itu, metode ini menyederhanakan pengelolaan kunci publik dapat didistribusikan dengan aman tanpa membahayakan kunci privat.

2. Analisis Keamanan Algoritma

a. Kecepatan Proses Enkripsi dan Deskripsi
   1) Jurnal 1: Perbandingan Kriptografi Simetris dan asimetris
   Algoritma kriptografi simetris seperti RC-5 dan AES memiliki keunggulan dalam hal kecepatan, baik saat melakukan enkripsi maupun dekripsi. Proses ini hanya memerlukan waktu dalam hitungan milidetik, menjadikannya sangat cocok untuk aplikasi yang membutuhkan pemrosesn data secara instan.
   2) Jurnal 2: Implementasi AES-128
   Hasil pengujian menunjukkan bahwa algoritma AES-128 mampu mengenkripsi data dengan sangat cepat. Hal ini menjadikannya pilihan ideal dalam sistem registrasi pasien, di mana waktu respons yang cepat sangat penting untuk akses data yang efisien.
   3) Pendekatan Hibrid Dengan memadukan enkripsi simetris untuk efisiensi dan enkripsi asimetris untuk pengelolaan kunci, sistem ini mampu mempertahankan kecepatan pemrosesan tinggi sekaligus menjaga tingkat keamanan yang optimal.

b. Tingkat Keamanan
   1) Jurnal 1: Analisis Kekuatan KeamananAlgoritma simetris seperti AES dan RC-5 memiliki panjang kunci yang cukup besar (128bit atau lebih), yang membuatnya tahan terhadap serangan brute force karena jumlah kombinasi yang harus diuji sangat banyak. Di sisi lain, kriptografi asimetris lebih unggul dalam melindungi

data dari serangan man-in-the-middle karena distribusi kunci publik tidak mengungkapkan kunci privat.

2) Jurnal 2: Keamanan AES-128AES-128 terbukti memiliki tingkat keamanan yang tinggi melalui berbagai pengujian. Panjang kuncinya membuat upaya brute force menjadi sangat tidak efektif, sehingga data tetap aman dari akses tidak sah.
3) Jurnal 3: Pendekatan HibridPendekatan gabungan antara kriptografi simetris dan asimetris meningkatkan proteksi secara menyeluruh. Kunci simetris yang digunakan untuk mengenkripsi data dilindungi oleh kriptografi asimetris, khususnya melalui kunci publik, yang mencegah risiko serangan selama proses pengiriman data. Selain itu, metode ini menyederhanakan pengelolaan kunci karena kunci publik dapat didistribusikan dengan aman tanpa membahayakan kunci privat.

c. RSA (Rivest-Shamir-Adleman)

Kelebihan:

Keamanan Komunikasi: Sebagai algoritma asimetris, RSA menggunakan pasangan kunci publik dan privat untuk menjamin keamanan komunikasi. Hal ini memungkinkan pertukaran informasi secara aman tanpa perlu membagikan kunci secara langsung (lihat Jurnal 1).

Distribusi Kunci yang Aman: Kunci publik dapat disebarluaskan tanpa risiko, memungkinkan pengguna lain untuk mengenkripsi pesan yang hanya bisa dibuka oleh pemilik kunci privat, sehingga mengurangi kemungkinan serangan man-in-the-middle.

Kekurangan:

Lambat dalam Pemrosesan: RSA memiliki kecepatan yang lebih rendah dibanding algoritma simetris seperti AES, terutama saat digunakan untuk mengenkripsi data dalam jumlah besar (lihat Jurnal 3).

Ukuran Kunci Lebih Besar: Untuk mencapai tingkat keamanan yang setara dengan AES, RSA memerlukan panjang kunci yang lebih besar, yang berdampak pada performa dan efisiensi sistem secara keseluruhan.

d. AES (Advanced Encryption Standard)

Kelebihan:

Cepat dan Efisien: AES dikenal memiliki kecepatan tinggi dalam proses enkripsi maupun dekripsi, menjadikannya sangat cocok untuk aplikasi yang memerlukan pemrosesan data secara real-time, seperti sistem pendaftaran pasien (lihat Jurnal 2).

Tingkat Keamanan Tinggi: Dengan opsi panjang kunci 128, 192, atau 256 bit, AES mampu memberikan perlindungan kuat terhadap serangan brute force.

Standar Global: AES telah digunakan secara luas dan diakui secara internasional sebagai standar enkripsi, sehingga dipercaya dalam berbagai bidang industri.

Kekurangan:

Bersifat Simetris: Karena menggunakan kunci yang sama untuk enkripsi dan dekripsi, manajemen kunci dalam AES menjadi tantangan tersendiri, khususnya dalam sistem dengan banyak pengguna yang memerlukan distribusi kunci secara aman (lihat Jurnal 1).

Risiko dalam Distribusi Kunci: Jika kunci dibocorkan atau dicuri, data terenkripsi dapat diakses dengan mudah oleh pihak yang tidak berwenang, sehingga meningkatkan potensi ancaman keamanan.

e. Sistem Hibrid: Kombinasi AES dan RSA untuk kinerja dan Keamanan Maksimal

1) Gambaran Umum Sistem HibridSistem hibrid merupakan pendekatan yang menggabungkan dua jenis algoritma kriptografi — yaitu AES (Advanced Encryption Standard) sebagai metode simetris dan RSA (Rivest-Shamir-Adleman) sebagai metode asimetris — guna menciptakan keseimbangan antara efisiensi dan

tingkat keamanan yang tinggi.

2) Penerapan dalam Aplikasi Nyata Pemanfaatan AES untuk Enkripsi Data AES digunakan untuk mengenkripsi data penting yang membutuhkan proses cepat, seperti data pribadi pasien pada sistem pendaftaran. Karena AES merupakan algoritma simetris, ia mampu mengenkripsi data dengan sangat efisien, menjadikannya ideal untuk aplikasi yang membutuhkan waktu tanggap singkat (seperti dijelaskan dalam Jurnal 2).
   a) RSA sebagai Pengaman Kunci Enkripsi
      RSA digunakan untuk mengamankan kunci AES. Kunci publik RSA dibagikan ke pengguna atau sistem yang berwenang, sedangkan kunci privat disimpan secara aman. Dengan pendekatan ini, meskipun data sudah dienkripsi dengan AES, hanya pihak dengan kunci privat RSA yang bisa mengakses kunci AES untuk mendekripsinya (mengacu pada Jurnal 3).
3) Keunggulan Pendekatan Gabungan ini
   a) Kinerja yang Optimal
      Dengan memanfaatkan AES untuk proses enkripsi data, sistem menjadi lebih cepat dan efisien. Hal ini sangat bermanfaat untuk aplikasi yang membutuhkan kecepatan tinggi, seperti transaksi waktu nyata (real-time), sebagaimana dibahas dalam Jurnal 1.
   b) Tingkat Keamanan yang Tinggi
      Kombinasi dua algoritma ini menghadirkan sistem yang tidak hanya cepat tetapi juga aman. Data yang dikodekan dengan AES tetap terlindungi selama pengiriman, karena kunci enkripsinya dijaga oleh mekanisme RSA. Strategi ini mengurangi risiko dari serangan seperti man-in-the-middle (lihat Jurnal 3).
   c) Manajemen Kunci yang Lebih Efisien dan Aman
      Penggunaan RSA untuk mengamankan kunci simetris AES membantu mengatasi kendala distribusi kunci dalam kriptografi simetris. Dengan demikian, pengelolaan kunci menjadi lebih mudah dan aman (berdasarkan Jurnal 1).

KESIMPULAN

1. Peran Algoritma Enkripsi dalam Keamanan Sistem Informasi:

Algoritma kriptografi memiliki fungsi vital dalam menjaga keamanan sistem informasi. Seiring meningkatnya risiko terhadap data sensitif, penerapan metode enkripsi yang efektif menjadi sangat penting untuk memastikan kerahasiaan, keutuhan, dan keaslian data. Ketiga jurnal yang dikaji menunjukkan bahwa penggunaan enkripsi yang tepat dapat secara signifikan mengurangi kemungkinan akses ilegal dan ancaman siber.

2. Relevansi AES dan RSA sebagai Algoritma Utama:

AES dan RSA tetap menjadi pilihan utama dalam dunia kriptografi karena kombinasi antara efisiensi dan perlindungan yang ditawarkan. AES dikenal dengan kecepatannya dalam mengenkripsi data, sementara RSA unggul dalam aspek keamanan komunikasi dan pengelolaan kunci. Ketika dikombinasikan dalam sistem hibrid, kedua algoritma ini saling melengkapi untuk menciptakan sistem yang andal dan aman.

Saran

1. Pemanfaatan Pendekatan Kombinasi Algoritma:

Para pengembang disarankan untuk menerapkan pendekatan kombinasi (hybrid) dalam sistem keamanan informasi mereka. Dengan menggabungkan kecepatan AES dan ketangguhan RSA, sistem yang dibangun akan lebih optimal—baik dari sisi kinerja maupun keamanan. Strategi ini dapat memberikan perlindungan maksimal terhadap data dari

berbagai jenis ancaman.

2. Peningkatan Literasi Pengguna tentang Keamanan Data:

Selain penerapan teknologi, penting juga untuk meningkatkan pemahaman pengguna akhir tentang pentingnya enkripsi data. Edukasi mengenai perlindungan informasi pribadi dan penggunaan sistem yang aman dapat membantu meningkatkan kesadaran akan keamanan digital. Kesadaran ini berperan penting dalam menjaga keamanan data pribadi serta memperkuat keamanan sistem secara keseluruhan.

DAFTAR PUSTAKA

Arif, Z., & Nurokhman, A. (2023). Analisis Perbandingan Algoritma Kriptografi Simetris dan Asimetris dalam Meningkatkan Keamanan Sistem Informasi. Jurnal Teknologi Sistem Informasi, 4(2). https://doi.org/10.35957/jtsi.v4i2.6077

Ramadhani, T. A., Cobantoro, A. F., & Sugianti. (2024). Implementasi Algoritma Advanced Encryption Standard 128 untuk Pengamanan Database Sistem Registrasi Pasien. Jurnal Informatika Polinema, 10(4). https://doi.org/10.33795/jip.v10i4.5619

Ridho, A., & Romli, M. A. (2024). Sistem Pengamanan Dokumen Menggunakan Algoritma Kriptografi Advanced Encryption Standard (AES-256). Jurnal Informatika Teknologi dan Sains (Jinteks), 6(4). https://doi.org/10.51401/jinteks.v6i4.4887