BAB I
PENDAHULUAN

1.1 Latar Belakang

Perkembangan teknologi informasi dan komunikasi yang sangat cepat dan pesat, telah mempengaruhi setiap sendi kehidupan manusia. Teknologi informasi telah menjadi bagian penting dalam kehidupan modern, dan memberikan kemudahan dalam berkomunikasi dan bertukar informasi. Namun, keamanan informasi menjadi hal yang sangat penting dalam dunia digital saat ini. Mengirim dan menerima berkas dari satu pihak ke pihak yang lain, seringkali dilakukan dalam kehidupan sehari-hari. Namun, tidak jarang berkas yang dikirim berhasil dicuri atau disadap oleh pihak yang tidak bertanggung jawab, dan ini bisa menyebabkan kerugian yang besar bagi kedua belah pihak, terutama jika data yang dikirim sangat penting dan rahasia. Oleh karena itu, diperlukan suatu metode pengamanan data yang efektif.

Saat ini penting bagi perusahaan/istansi dalam mengamankan file teks. Hal ini terkait dengan perlindungan data rahasia, kepatuhan terhadap regulasi yang ketat, menjaga reputasi dan kepercayaan mitra/pelanggan, serta memastikan integritas data. Selain itu, keamanan data teks memungkinkan perusahaan untuk berbagi informasi dengan mitra bisnis dan pihak ketiga dengan aman, mengatur akses data, dan melindungi diri dari ancaman keamanan *cyber* yang terus berkembang. Dalam dunia bisnis yang serba digital ini, mengamankan data teks adalah langkah penting dalam menjaga keberlanjutan dan keberhasilan perusahaan.

Salah satu metode kriptografi yang digunakan dalam pengamanan data adalah algoritma RSA (Rivest Shamir Adleman). Algoritma ini merupakan metode kriptografi yang menggunakan kunci private dan kunci public untuk proses enkripsi dan dekripsi data [1] (Graham, S L, 1978). Algoritma RSA menggunakan kunci private untuk melakukan enkripsi dan kunci public untuk dekripsi, sehingga seringkali disebut sebagai teknik kriptografi asimetris.

Dalam penelitian ini, penulis akan menerapkan algoritma kriptografi RSA pada pengamanan file text. Enkripsi dan deskripsi data akan dilakukan

menggunakan algoritma RSA, dengan menghasilkan dua kunci yang berbeda untuk setiap prosesnya. Diharapkan dengan menggunakan algoritma RSA, data yang dikirimkan dapat terlindungi dan tidak dapat dicuri atau disadap oleh pihak yang tidak bertanggung jawab.

Penggunaan algoritma kriptografi RSA sebagai metode pengamanan data dalam konteks perkembangan teknologi informasi dan komunikasi yang sangat cepat memiliki beberapa alasan yang kuat, berikut adalah alsan pengunaan algoritma kriptografi RSA:

1. Algoritma RSA merupakan salah satu teknik kriptografi asimetris yang paling terkenal. Dalam kriptografi asimetris, ada dua kunci yang berbeda, yaitu kunci publik dan kunci pribadi. Kunci publik digunakan untuk enkripsi, sedangkan kunci pribadi digunakan untuk dekripsi. Hal ini membuatnya sangat cocok untuk skenario di mana banyak pihak perlu berkomunikasi dengan aman, seperti dalam pengiriman berkas atau pesan yang harus dienkripsi oleh pengirim dan didekripsi oleh penerima.
2. Algoritma RSA dikenal dengan tingkat keamanan yang tinggi. Keamanan algoritma ini didasarkan pada kesulitan dalam memfaktorkan bilangan-bilangan besar. Dalam kata lain, menghitung kunci pribadi dari kunci publik sangat sulit dan memerlukan waktu yang sangat lama, terutama jika bilangan-bilangan tersebut sangat besar. Oleh karena itu, algoritma RSA memberikan tingkat keamanan yang tinggi terhadap serangan brute-force.
3. RSA dapat digunakan dalam berbagai aplikasi, dari mengamankan pengiriman email hingga melindungi informasi transaksi online. Algoritma ini dapat diimplementasikan dalam berbagai platform dan perangkat lunak dengan relatif mudah, sehingga sangat skalabel untuk berbagai kebutuhan dalam hal ini kriptografi RSA digunakan sebagai pengamanan file teks.
4. Algoritma RSA telah digunakan secara luas dalam berbagai aplikasi dan telah terbukti efektif. Ini telah menjadi salah satu standar industri dalam kriptografi asimetris, dan banyak sistem keamanan mengandalkan algoritma ini untuk melindungi data sensitif.

5. Algoritma RSA dapat diimplementasikan dengan relatif mudah menggunakan perangkat lunak yang tersedia secara luas. Ini membuatnya dapat digunakan oleh banyak orang dan organisasi tanpa perlu membangun sistem kriptografi yang rumit dari awal.

Dengan memanfaatkan algoritma kriptografi RSA, penulis dapat memastikan bahwa data teks yang dikirimkan aman dari pencurian atau penyadapan oleh pihak yang tidak berwenang.

1.2 Rumusan Masalah

Berdasarkan penjelasan dari latar belakang di atas, maka perumusan masalah yang akan dibahas adalah sebagai berikut:

1. Bagaimana merancang keamanan file teks menggunakan Algoritma Rivest-Shamir-Adleman (RSA)?
2. Apakah Algoritma Rivest-Shamir-Adleman (RSA) dapat digunakan dalam mengamankan file teks?

1.3 Batasan Masalah

Batasan masalah dalam penelitian ini adalah sebagai berikut:

1. Penelitian ini membahas penggunaan Algoritma Rivest Shamir Adleman (RSA)". untuk mengkompresi isi file teks dan algoritma RSA untuk mengamankan hasil kompresi.
2. Format file yang digunakan adalah *.docx dan *.txt
3. Karakter yang digunakan berdasarkan pada tabel American Standard Code for Information Interchange (ASCII).
4. Tidak melakukan kompresi-dekompresi dan enkripsi-dekripsi terhadap komponen lain seperti tabel atau gambar yang terdapat di dalam file teks.

1.4 Tujuan Penelitian

Berikut adalah tujuan dari penelitian ini :

1. Penelitian ini bertujuan untuk menganalisis tingkat keamanan data yang dihasilkan oleh Algoritma Rivest Shamir Adleman (RSA). Melalui analisis ini, akan dievaluasi sejauh mana algoritma ini dapat melindungi data dari ancaman keamanan seperti peretasan dan

pengungkapan yang tidak sah.

2. Penelitian ini akan menyelidiki dan memahami prinsip dasar dari Algoritma RSA. Dalam konteks ini, akan dilakukan studi mendalam tentang bagaimana kunci publik dan kunci pribadi digunakan dalam algoritma ini untuk enkripsi dan dekripsi data.
3. Penelitian ini akan merancang dan mengimplementasikan sistem keamanan data yang menggunakan Algoritma RSA. Ini melibatkan penerapan langkah-langkah enkripsi dan dekripsi RSA yang benar untuk melindungi integritas dan kerahasiaan data yang ditransmisikan melalui jaringan atau disimpan dalam penyimpanan.
4. Penelitian ini akan mengevaluasi kinerja Algoritma RSA dalam konteks keamanan data. Akan dilakukan analisis terhadap kecepatan enkripsi dan dekripsi, kekuatan keamanan, dan efisiensi penggunaan sumber daya yang terkait dengan implementasi algoritma ini.

1.5 Manfaat Penelitian

Penelitian ini memiliki beberapa manfaat, antara lain sebagai berikut :

1. Penelitian ini diharapkan dapat meningkatkan keamanan data dengan menerapkan Algoritma Rivest Shamir Adleman (RSA) pada hasil kompresi file teks. Dengan menggunakan algoritma kriptografi yang kuat seperti RSA, pesan yang dihasilkan dari kompresi file teks akan terlindungi secara efektif dari ancaman kebocoran atau pengungkapan yang tidak sah.
2. Dengan mengamankan isi dari hasil kompresi file teks menggunakan Algoritma RSA, penelitian ini dapat memastikan bahwa komunikasi antara pengirim dan penerima pesan tetap aman. Pesan yang dikompresi dan dienkripsi dengan menggunakan RSA hanya dapat dibaca oleh penerima yang memiliki kunci pribadi yang sesuai, sehingga informasi sensitif dalam pesan tetap terjaga kerahasiaannya.

3. Penelitian ini diharapkan dapat memberikan kontribusi pada pengembangan keamanan informasi dengan menerapkan dan menganalisis Algoritma RSA dalam konteks kompresi file teks. Hasil penelitian ini dapat memberikan wawasan dan pemahaman yang lebih baik tentang penggunaan RSA dalam menjaga kerahasiaan pesan, sehingga dapat digunakan sebagai acuan dan panduan dalam pengembangan sistem keamanan data yang lebih kuat dan terpercaya.

1.6 Sistematika Penulisan

Skripsi ini disusun dalam rangka menyajikan hasil penelitian yang dilakukan.

Pendahuluan dimulai dengan latar belakang penelitian untuk menggambarkan konteks dan alasan pemilihan topik. Selanjutnya, Rumusan masalah digunakan untuk mengidentifikasi permasalahan yang akan diselesaikan. Tujuan penelitian disampaikan untuk menjelaskan tujuan yang ingin dicapai melalui penelitian ini. Manfaat penelitian dijelaskan untuk menggambarkan manfaat penelitian ini dalam pengembangan ilmu pengetahuan dan praktik terkait.

Dalam tinjauan pustaka, terdapat studi literatur dan dasar teori. Studi literatur mencakup penelitian-penelitian yang sudah dilakukan sebelumnya. Pada bagian ini, peneliti memberikan tinjauan umum tentang topik penelitian, merangkum penelitian-penelitian terkait, dan menyoroti temuan utama, metodologi, dan hasil dari penelitian-penelitian tersebut. Sementara itu, bagian dasar teori menjelaskan dasar teoretis yang digunakan dalam penelitian. Pada bagian ini, peneliti menjelaskan teori-teori yang relevan dengan topik penelitian, konsep-konsep yang terkait

Metode penelitian meliputi alur penelitian, dan alat dan bahan yang digunakan. Alur penelitian menjelaskan langkah-langkah yang akan diambil dalam penelitian. Alat dan bahan menjelaskan tentang peralatan, instrumen

yang akan digunakan dalam penelitian.

Hasil dan pembahasan mencakup beberapa komponen penting, seperti analisis sistem berjalan, diagram, kamus data, struktur tabel, dan pengujian sistem. Analisis sistem berjalan dilakukan untuk mengetahui permasalahan yang sebenarnya. Diagram digunakan untuk memvisualisasikan struktur dan alur sistem. Pengujian sistem merupakan tahap evaluasi dan verifikasi terhadap sistem yang telah dikembangkan.

Kesimpulan memberikan ringkasan dari hasil penelitian yang telah dilakukan. Sedangkan saran menjelaskan bagian yang memberikan rekomendasi dan panduan untuk penelitian selanjutnya atau pengembangan lebih lanjut. Referensi dalam penulisan mencakup berbagai sumber yang digunakan, seperti buku, jurnal, artikel, dan sumber elektronik.