BAB 1
PENDAHULUAN

1.1 Latar Belakang

Keamanan dan kerahasiaan merupakan salah satu aspek yang paling penting pada suatu sistem pesan, data dan informasi. Masalah tersebut masih kurang diperhatikan dari para perancang dan pengelola sistem informasi sehingga masalah keamanan berada di bagian terakhir setelah tampilan. Ilmu yang mempelajari tentang cara-cara mengamankan data atau pesan dikenal dengan istilah Kriptografi, sedangkan dalam langkah-langkah kriptografi disebut algoritma kriptografi. Berdasarkan kunci yang digunakan, algoritma kriptografi dapat dibagi menjadi dua, yaitu algoritma simetrik dan algoritma asimetrik. Dimana algoritma simetrik menggunakan satu kunci untuk proses enkripsi dan dekripsinya. Sedangkan algoritma asimetrik menggunakan dua kunci berbeda untuk proses enkripsi dan dekripsinya, yaitu kunci umum *(public key)* yang digunakan untuk proses enkripsi yaitu perubahan data teks asli *(plain text)* menjai teks rahasia *(chiper text)* yang sifatnya tidak rahasia dan kunci pribadi *(private key)* yang digunakan untuk proses dekripsinya yaitu pengambilan data teks rahasia *(chipr text)* menjadi teks asli *(plain text)* yang sifatnya rahasia dan masing-masing pihak memiliki kunci pribadi yang berbeda. (Kristoforus, Aditya. 2012)

Pada jurnal Hendri Syahputra yang berjudul “Aplikasi Enkripsi data file teks dengan Algoritma RSA (Rivest Shamir Adleman)” berhasil mengamankan file teks untuk dienkripsi dan dekripsi menggunakan algoritma RSA (Rivest Shamir Adleman), tetapi hanya dapat mengenkripsi dan dekripsi file teks yang

panjangnya tidak lebih dari 1000 karakter. Jurnal tersebut yang menjadikan acuan untuk penelitian pertama

Pada jurnal Andi Riski Alvianto yang berjudul “Pengaman Pengiriman Pesan via SMS dengan algoritma RSA berbasis android” berhasil membuktikan bahwa algoritma RSA tidak hanya digunakan untuk keamanan data dan digital signature, tetapi metode ini juga dapat digunakan untuk keamanan pesan teks dengan waktu rata-rata proses enkripsi yaitu 14,925 milisecond per karakter dan dekripsi 4,679 milisecond per karakter, Jurnal tersebut yang menjadikan acuan untuk penelitian kedua.

(RSA) adalah salah satu algoritma kriptografi asimetris (kriptografi kunci-publik) yaitu menggunakan dua kunci yang berbeda (*private key* dan *public key*). Kekuatan algoritma RSA tidak hanya terletak pada panjang kuncinya (semakin panjang kunci, maka semakin lama waktu kerja) dan penggunaan kunci-publik dan kunci privat pada umumnya. Kekuatan utama dari algoritma RSA didasarkan pada sulitnya memfaktorkan bilangan besar menjadi faktor-faktor prima : faktorkan n menjadi dua faktor prima, p dan q, sedemikian sehingga $n = p \cdot q$. RSA merupakan algoritma kriptografi asimetrik yang paling mudah untuk diimplementasikan dan dimengerti (Ariyus, 2008)

Pada proses pengiriman pesan terdapat beberapa hal yang harus diperhatikan, yaitu kerahasiaan, integritas, autentikasi, dan non repudiasi. Hal tersebut dibutuhkan suatu proses pengkodean atau penyandian sebelum dilakukan proses pengiriman. Sehingga proses pengiriman pesan yang dikirim terjaga

kerahasiaannya dan tidak dapat diubah untuk menjaga integritas pesan tersebut (Wirdasari, 2008).

Berdasarkan pemaparan dari jurnal yang ada, masalah yang terjadi adalah enkrip dan dekripsi pesan tidak lebih dari 1000 karakter dan memerlukan waktu enkripsi yaitu 14,925 milisecond per karakter dan dekripsi 4,679 milisecond per karakter. Oleh karena itu penulis bermaksud untuk melakukan penelitian dalam bentuk skripsi dengan topik **"IMPLEMENTASI KRIPTOGRAFI MENGGUNAKAN ALGORITMA RIVEST SHAMIR ADLEMAN (RSA) UNTUK KEAMANAN PESAN TEKS".**

1.2. Rumusan Masalah

Berdasarkan latar belakang yang ada, maka dapat diambil suatu rumusan masalah yaitu:

1. Bagaimana penerapan algoritma kriptografi RSA untuk keamanan pesan text?
2. Bagaimana proses enkripsi dan dekripsi pesan teks lebih dari 1000 karakter yang lebih efesien waktu?

1.3. Tujuan Penelitian

Berdasarkan latar belakang dan rumusan masalah yang telah dibahas sebelum nya, maka tujuan penelitiannya yaitu:

1. Menganalisis sistem keamanan pesan text yang ada, guna menerapkan sistem keamanan pesan text menggunakan algoritma kriptografi RSA .
2. Sistem ini diharapkan dapat membantu pengguna dalam keamanan pesan text yang cepat dalam mengenkripsi dan mendekripsikan sebuah pesan.

1.4. Batasan Masalah Penelitian

Berdasarkan latar belakang, rumusan masalah dan tujuan penelitian, maka batasan masalah penelitiannya yaitu:

1. Sistem keamanan pesan text dengan enkripsi dan dekripsi RSA .
2. Objek yang dibahas hanya pada ke efesiensi nya waktu yang dibutuhkan untuk enkrip dan dekrip pesan lebih dari 1000 karakter.

1.5 Manfaat penelitian

Adapun manfaat penelitian ini adalah sebagai berikut:

1. Manfaat Bagi Pengguna:

   Memberikan keamanan pesan text dengan enkripsi dan dekripsi RSA yang lebih efesien

2. Manfaat Bagi Mahasiswa:

   Sebagai sarana pelatihan dalam menyusun, membahas dan memecahkan suatu masalah yang ada.

1.6 Sistematika Penulisan

BAB I Pendahuluan

Latar Belakang Masalah, Rumusan Masalah, Tujuan Penelitian, Batasan Masalah, Manfaat Penelitian, Sistematika Penulisan.

BAB II Landasan Teori

Tinjauan Pustaka, Implementasi, Kriptografi, Algoritma, Konsep Dasar Perhitungan Matematis, Pengertian Keamanan, Pengertian Pesan Teks, Perangkat Lunak yang Digunakan, Bagan Alir Dokumen (BAD).

BAB III Metode Penelitian

Kerangka Pemikiran, Tahapan Penelitian, Alat yang digunakan dalam penelitian, Rancangan Arsitektur Sistem, Proses Pembuatan Kunci, Proses Enkripsi, Proses Dekripsi, Pemfaktoran Metode Kraitchik.

BAB IV Implementasi

Perhitungan Kriptografi dengan Metode RSA, Implementasi Program, Pengujian Program, Penjadwalan.

BAB V Simpulan dan Saran

Simpulan, Saran

DAFTAR PUSTAKA

LAMPIRAN