BAB I

PENDAHULUAN

1.1 Latar Belakang

Jaringan komputer mempunyai peranan yang penting dalam era globalisasi informasi sekarang ini. Penggunaan jaringan komputer telah meluas ke dalam sektor-sektor kehidupan manusia, misalnya dalam bidang perbankan, industri sampai militer, karena jaringan komputer bersifat *Resource Sharing* atau berbagi penggunaan informasi. *Resource Sharing* memudahkan pengguna jaringan berbagi informasi tanpa dipengaruhi oleh lokasi sumber informasi dan pengguna sehingga seorang pengguna dapat memperoleh informasi yang dibutuhkan dengan mudah. Jaringan komputer juga memberikan kemudahan kepada antar pengguna untuk saling mengirim informasi, tetapi terdapat resiko yang harus ditanggung oleh pengguna, misalnya penyadapan oleh orang yang tidak berhak atau penyusup. Oleh sebab itulah diperlukan keamanan dalam pemanfaatan jaringan komputer untuk menghindarkan pengguna dari resiko yang dapat timbul seperti penyadapan, penipuan dan pemalsuan.

Keamanan jaringan komputer digunakan untuk mencegah akses dari pihak yang tidak berhak atau penyusup sehingga resiko yang harus ditanggung oleh pengguna dapat dihindari terutama pada informasi yang bersifat rahasia. Keamanan jaringan komputer memberi keyakinan kepada pengguna bahwa penyusup tidak mungkin dapat membaca, atau lebih buruk lagi, dapat mengubah informasi yang bersifat rahasia tersebut. Sehingga dapat dikatakan bahwa keamanan jaringan komputer berhubungan dengan cara untuk mengamankan

suatu informasi yang bersifat rahasia yang akan dikirim kepada penerima. Salah satu cara yang dapat dilakukan untuk menjaga kerahasiaan suatu informasi adalah dengan cara menyandikan informasi tersebut.

Cabang ilmu yang mempelajari tentang persandian disebut Kriptologi. Kriptologi terdiri atas dua bagian yaitu Kriptografi dan Kriptanalisis. Kriptografi adalah seni untuk mengamankan plainteks dengan menggunakan teknik penyandian. Kriptanalisis adalah seni untuk memecahkan sandi. Dalam kriptografi terdapat sistem kriptografi yang disebut dengan Kriptosistem. Dalam kriptosistem, melibatkan dua pihak yaitu pihak pengirim dan penerima. Pengirim akan mengubah informasi asli yang disebut dengan Plainteks sebelum mengirimkannya kepada penerima. Proses penyandian plainteks disebut dengan Enkripsi sedangkan informasi yang didapatkan dari proses enkripsi disebut dengan Ciperteks. Penerima kemudian akan menguraikan ciperteks untuk mendapatkan kembali plainteks. Proses penguraian ciperteks disebut dengan Dekripsi. Dalam proses enkripsi dan dekripsi digunakan suatu fungsi dengan menggunakan suatu kunci untuk menjaga kerahasiaan informasi.

Mengingat ciperteks dikirim melalui saluran komunikasi atau *chanel* yang tidak dapat dijamin keamanannya, terdapat suatu alternatif dengan menggunakan kriptosistem yang kunci enkripsi dan kunci dekripsinya berbeda. Metode tersebut dikenal dengan istilah Kriptosistem Kunci Umum (*Public Key Cryptosystem*). Dalam Kriptosistem Kunci Umum, setiap pengguna mempunyai dua kunci yaitu kunci enkripsi yang bersifat publik atau umum dan kunci dekripsi yang bersifat rahasia. Kunci enkripsi merupakan kunci yang dapat diketahui oleh

semua pengguna Kriptosistem Kunci Umum sedangkan kunci dekripsi merupakan kunci yang harus dijaga kerahasiaannya oleh setiap pengguna.

Salah satu algoritma yang dapat digunakan dalam Kriptosistem Kunci Umum adalah Algoritma Rivest-Shamir-Adleman (RSA). Algoritma RSA adalah algoritma penyandian yang didasarkan pada prinsip-prinsip teori bilangan. Algoritma RSA menggunakan bilangan dari mulai pemilihan kunci-kunci yang digunakan yaitu kunci enkripsi dan kunci dekripsi sampai ciperteks yang dihasilkan.

Dalam algoritma RSA, setiap karakter dalam plainteks terlebih dahulu akan dikonversi atau diubah ke dalam bentuk bilangan sebelum dienkripsikan. Sehingga dibutuhkan suatu sumber kode yang akan digunakan dalam konversi plainteks tersebut. Keamanan algoritma RSA terletak pada pemfaktoran bilangan yang sampai saat ini belum dapat ditemukan suatu algoritma pemfaktoran bilangan yang efisien.

1.2 Perumusan Masalah

Permasalahan dalam penulisan tugas akhir adalah penggunaan algoritma RSA dalam Kriptosistem Kunci Umum. Pembahasan dari permasalahan meliputi :

1. Menerapkan kriptografi dalam sistem keamanan informasi.
2. Mengenkripsi dan mendekripsi suatu plainteks dengan menggunakan algoritma RSA .
3. Mengimplementasi algoritma RSA dalam bahasa pemograman Pascal 7.0.

1.3 Pembatasan Masalah

Penulisan tugas akhir ini dibatasi pada penggunaan algoritma RSA dengan sumber kode yang digunakan dalam konversi plainteks ke dalam bentuk bilangan dan sebaliknya adalah himpunan karakter dalam kode *ASCII* (*American Standard Code Information Interchange*) mulai karakter nomor kode *ASCII* 32 sampai 126 dengan nomer kode yang telah dimodifikasi menjadi nomor kode 01 sampai 95. Implementasi algoritma RSA dilakukan dengan menggunakan plainteks yang berupa file berecord dan mengabaikan tingkat pengiriman . Tiap record pada file plainteks dibatasi sampai 126 karakter dengan jumlah record maximal 50 record. Nilai eksponen enkripsi dalam kunci publik RSA dipilih dengan nilai terkecil.

1.4 Sistematika Penulisan

BAB I berisikan latar belakang, perumusan masalah, pembatasan masalah dan sistematika penulisan

BAB II berisikan teori dasar meliputi fungsi, teori bilangan, sistem bilangan biner dan file.

BAB III berisikan pembahasan meliputi kriptografi, konsep dasar kriptografi, Kriptosistem Kunci Umum, algoritma Rivest- Shamir-Adleman (RSA) dan implementasi algoritma Rivest- Shamir-Adleman (RSA).

PENUTUP

DAFTAR PUSTAKA

LAMPIRAN