BAB I
PENDAHULUAN

1.1 Latar Belakang Masalah

Dunia jaringan telekomunikasi kini berkembang begitu pesat. Saat ini perkembangan tidak hanya pada jalur komunikasi suara, namun juga pada jalur komunikasi data. Dalam pengiriman data dibutuhkan proses pengamanan agar data yang dikirim aman sampai pada penerima.

Untuk menunjang kebutuhan akan proses pengamanan ini, salah satu caranya adalah dengan menggunakan proses enkripsi pada data yang dikirim. Dengan menggunakan proses ekripsi, pengirim bisa menjaga kerahasiaan pesan yang dikirimnya agar tidak diketahui oleh orang lain selain penerima. Pada dasarnya proses pengamanan mengunakan algoritma enkripsi RSA sudah baik, namun masih memiliki beberapa kekurangan. Beberapa diantaranya adalah jika menggunakan kunci yang pendek maka akan gampang difaktorkan dan terpisahnya proses otentikasi terhadap proses enkripsi yang dapat mengakibatkan kesamaan ciphertext yang diterima dari hasil enkripsi siapa saja.

Oleh karena itu pada Tugas Akhir ini dilakukan perancangan sistem pengamanan dan otentikasi pengiriman pesan menggunakan modifikasi algoritma enkripsi asimetri RSA. Modifikasi yang akan digunakan berupa gabungan fungsi modifikasi *n-prime* dalam pembangkitan kunci setiap user dan modifikasi penggabungan otentikasi dan enkripsi pada pesan yang akan dikirim.

1.2 Rumusan Masalah

Adapun rumusan masalah dalam Tugas Akhir ini adalah:

Bagaimana mekanisme modifikasi RSA dari sisi modifikasi *n-prime* dalam sistem pembangkitan kunci modifikasi algoritma RSA?

Bagaimana mekanisme modifikasi penggabungan proses otentikasi dan proses enkripsi pada sistem enkripsi dan dekripsi modifikasi RSA?

Bagaimana perbandingan kinerja sistem enkripsi modifikasi RSA yang dirancang dengan kinerja sistem enkripsi RSA tanpa modifikasi dan sistem RSA dengan penyisipan otentikasi hash?

1.3 Batasan Masalah

Adapun batasan masalah dalam Tugas Akhir ini adalah:

1. Masukan sistem dibatasi hanya berupa pesan text (huruf, angka).
2. Masukan sistem dibatasi hanya berupa karakter pada tabel ASCII

1.4 Tujuan dan Manfaat

Adapun tujuan dan manfaat dari Tugas Akhir ini adalah:

1. Mengetahui mekanisme modifikasi RSA dari sisi modifikasi *n-prime* dalam sistem pembangkitan kunci modifikasi algoritma RSA.
2. Mengetahui mekanisme modifikasi penggabungan proses otentikasi dan proses enkripsi pada sistem enkripsi dan dekripsi modifikasi RSA.
3. Menganalisis kinerja sistem enkripsi enkripsi modifikasi RSA yang dirancang dengan kinerja sistem enkripsi RSA tanpa modifikasi dan sistem RSA dengan penyisipan otentikasi hash.

1.5 Metodologi

Adapun metodologi yang digunakan dalam Tugas Akhir ini adalah metodologi experimental, yang terdiri dari lima tahapan:

1. Tahap studi literatur.

   Pada tahap ini dilakukan pendalaman tentang konsep dan teori melalui pustaka-pustaka yang berkaitan dengan penelitian baik berupa buku, jurnal, dan lain-lainnya.

   Adapun literatur yang akan didalami adalah:

   a. Algoritma enkripsi asimetri RSA.
   b. Pendalaman teori dalam perancangan sistem enkripsi dan dekripsi menggunakan algoritma modified RSA.
   c. Literatur-literatur lainnya yang mendukung.

2. Tahap perancangan sistem.

   Pada tahap ini dilakukan desain model system yang sesuai dengan kriteria spesifikasi sistem berdasarkan dari hasil studi literatur.

3. Tahap simulasi.

   Pada tahap ini dilakukan simulasi sistem yang telah dirancang.

4. Tahap analisis.

Pada tahap ini dilakukan analisa terhadap hasil simulasi sistem.

5. Tahap pembuatan laporan.

Pada tahap ini dilakukan penyusunan laporan dari Tugas Akhir ini dan pengumpulan dokumentasi yang diperlukan. Format laporan akan mengikuti kaidah penulisan yang benar dan sesuai dengan ketentuan-ketentuan yang telah ditetapkan oleh institusi.

1.6 Penelitian Terdahulu

Beberapa penelitian yang dilakukan sebelumnya yangtelah dilakukan mengenai algoritma RSA

1. Penelitian yang dilakukan oleh amare ayale anagaw mengenai 'A Modified RSA Encription Tecnique Based on Multiply public keys' [1]
2. Penelitian yang dilakukan oleh B Ivy Persis Urbana mengenai 'A modified RSA Criptosystem Based on 'n' Prime Number' [3]

Kedua penilitian tersebut tidak melakukan modifikasi penggabungan proses otentikasi dalam sistem enkripsi dan dekripsi.