BAB I

PENDAHULUAN

1.1 Latar Belakang Masalah

Teknologi informasi dan komunikasi saat ini berkembang demikian pesat khususnya internet. Perkembangan teknologi internet berdampak meningkatnya penggunaan internet sebagai media komunikasi, transfer data hingga transaksi kuangan. Disamping itu terdapat kekurangan dan cenderung tidak aman *(unreliable)*, karena banyak celah yang dapat dimanfaatkan oleh pihak-pihak yang tak berwenang untuk mengakses sebuah data untuk disalahgunakan. Oleh karena itu, keamanan menjadi faktor utama yang harus dipenuhi.

Permasalahan keamanan data ini dapat diatasi dengan menggunakan kriptografi yang bertujuan memberi layanan keamanan seperti kerahasiaan, integritas data, otentikasi, dan nirpenyangkalan. Kriptografi merupakan bidang pengetahuan yang menggunakan persamaan matematis untuk melakukan proses enkripsi maupun dekripsi data. Teknik ini digunakan untuk mengubah data ke dalam kode-kode tertentu, dengan tujuan informasi yang disimpan atau ditransmisikan melalui jaringan yang tidak aman (misalnya saja internet) tidak dapat dibaca oleh siapapun kecuali orang-orang yang berhak.

Konsep kriptografi kunci publik baru muncul pada tahun 1976. berawal dari gagagsan para penemunya, Whitfield Diffie dan Martin Hellman, dan secara terpisah oleh Ralph Merkle, bahwa kunci dapat berpasangan, yaitu kunci enkripsi dan kunci dekripsi dan hampir tidak mungkin untuk menghasilkan suatu kunci dari kunci yang lainnya. Beberapa kelemahan kriptografi kunci simetri dapat diselesaikan menggunakan kriptografi kunci publik, yaitu permasalahan distribusi kunci *(key exchange)* dan efisiensi jumlah kunci.

Terdapat tiga jenis utama kriptografi kunci publik yang berbasis pada teori bilangan komputasional yaitu: *Integer Factorization Problem (IFP), Discrete Logarithm Problem (DLP), dan High Degree Residuosity Class*. RSA adalah yang termasuk ke dalam kategori IFP, dibuat oleh Ron Rivest, Adi Shamir, dan Leonard Adleman pada tahun 1976. Sedangkan Elgamal termasuk ke dalam kategori DLP, dibuat oleh Taher ElGamal pada tahun 1984. Hal yang menarik dari kedua algoritma tersebut adalah bahwa keduanya berangkat dari dasar permasalahan yang berbeda (faktorisasi bilangan bulat dan logaritma diskret), namun dapat diaplikasikan untuk proses enkripsi dan tandatangan digital. Dengan demikian dapat memenuhi aspek kerahasiaan, otentikasi, dan sekaligus nirpenyangkalan *(non-repudiation)*.

1.2 Rumusan Masalah

Dari permasalahan di atas, maka dirumuskan untuk dibuat sebuah perangkat lunak aplikasi yang menerapkan algoritma

kriptografi kunci publik RSA dan Elgamal untuk menangani proses pembangkitan kunci, enkripsi, dekripsi, tandatangan digital, dan verifikasi, serta menampilkan beberapa grafik yang merepresentasikan kinerja masing-masing algoritma berdasarkan hasil pengujian terhadap setiap proses yang ditangani. Grafik tersebut akan dijadikan sebagai acuan analisis perbandingan antara kedua algoritma tersebut.

1.3 Ruang Lingkup

Ruang lingkup pada penelitian ini adalah sebagai berikut:

1. Penelitian ini membahas proses pembangkitan kunci, enkripsi dan tanda tangan digital pada algoritma RSA dan El Gamal.
2. Aplikasi yang dibangun akan menangani proses enkripsi, dekripsi, tandatangan digital dan verifikasi terbatas pada file teks saja.
3. Aplikasi dibangun menggunakan bahasa pemrograman JAVA dan UML sebagai bahasa pemodelannya.
4. Pengujian algoritma RSA dan El Gamal dilakukan menggunakan perangkat PC Pentium 4 2.8 GHz, 512 MB RAM untuk memproses beberapa file teks yang berbeda ukuran.
5. Perhitungan waktu pemrosesan ditangani kode program dengan mengambil waktu sistem tepat sebelum proses dimulai dan tepat setelah proses selesai, kemudian menghitung selisih waktunya.

1.4 Tujuan

Adapun tujuan dari penelitian ini adalah sebagai berikut:

1. Membangun program aplikasi untuk menjaga kerahasiaan dan otentikasi data atau informasi dengan menerapkan algoritma kunci publik RSA dan El Gamal.
2. Mengetahui perbandingan kinerja algoritma RSA dan El Gamal dalam melakukan proses pembangkitan kunci, enkripsi, tanda tangan digital, dan perbandingan ukuran cipher yang dihasilkan.