BAB III

METODOLOGI PENELITIAN

3.1. Masalah Keamanan Pesan

Salah satu metode untuk berkomunikasi adalah melalui tulisan. Tulisan berfungsi untuk menyampaikan pesan. Pesan yang terkandung dalam tulisan bisa berisi informasi rahasia maupun tidak. Informasi rahasia dapat terjaga keamanannya jika disampaikan oleh pemberi pesan secara langsung kepada penerima pesan. Namun jika pesan disampaikan secara tidak langsung melalui pihak ketiga maka informasi rahasia pada pesan tidak terjamin keamanannya. Salah satu cara yang dapat ditempuh untuk mengamankan pesan adalah dengan mengubahnya menjadi sandi-sandi yang sulit dibaca dan hanya bisa dibaca oleh pihak tertentu, metode ini disebut kriptografi.

3.2. Kriptografi RSA dan Kriptografi ElGamal

Algoritma kriptografi yang hingga saat ini masih banyak digunakan adalah algoritma RSA dan algoritma ElGamal. Kedua algoritma tersebut masih digunakan karena belum ada penyadap yang mampu memecahkannya. Dengan kata lain, kedua algoritma tersebut masih dianggap aman.

Kekuatan algoritma RSA terletak pada proses eksponensial dan pemfaktoran suatu bilangan menjadi dua bilangan prima yang hingga kini memerlukan waktu yang sangat lama bahkan hingga empat miliar tahun. Kelebihan lain dari algoritma ini adalah ketahanannya terhadap berbagai serangan, terutama serangan *brute force*. Kekuatan algoritma ElGamal adalah pada perhitungan logaritma diskrit pada modulo prima yang besar.

3.3. Pengembangan Kriptografi RSA dan Kriptografi ElGamal

Pengembangan kriptografi RSA dan kriptografi ElGamal dilakukan dengan menggabungkan kedua algoritma tersebut. Tujuannya agar diperoleh algoritma kriptografi baru yang tetap aman. Langkah pertama adalah dengan meningkatkan kecepatan algoritma kriptografi RSA melalui penambahan satu bilangan prima pada proses pembangkitan kunci. Setelah diperoleh algoritma RSA yang ditingkatkan, maka dilakukan penggabungan algoritma RSA yang ditingkatkan dengan algoritma ElGamal dengan cara menggabungkan proses pembangkitan kunci pada algoritma RSA yang ditingkatkan dan algoritma ElGamal kemudian dikonstruksi rumus enkripsi dan dekripsi yang memuat unsur-unsur kedua algoritma tersebut.

3.4. Konstruksi Program Aplikasi

Pembuatan program aplikasi dari algoritma kombinasi hasil penggabungan algoritma RSA yang ditingkatkan dengan algoritma Elgamal dilakukan dengan cara mengubah model matematis algoritma kombinasi ke dalam bahasa pemrograman. Program yang digunakan adalah Java NetBeans 8.2. Model yang dibuat dalam program aplikasi adalah proses pembangkitan kunci, enkripsi hingga dekripsi.

Pada program aplikasi yang akan dikonstruksi, diberikan pilihan bagi *user* (pengguna program) apakah sebagai pengirim pesan atau penerima pesan. Pada pilihan penerima pesan, diberikan pilihan kembali untuk membangkitkan kunci secara otomatis atau memasukkan kunci secara manual agar *user* memperoleh kunci yang tepat.

3.5. Validasi

Pada tahap validasi, dilakukan analisis pada model yang dikembangkan apakah proses enkripsi dan dekripsi sudah cocok atau belum cocok. Pada tahap ini, validasi yang dilakukan yaitu validasi terhadap program aplikasi yang dirancang.

Validasi ini dilakukan untuk menguji apakah program yang dirancang berdasarkan algoritma kombinasi sudah valid dan bisa digunakan dalam penyandian pesan atau tidak valid.

3.6. Kesimpulan

Setelah program aplikasi tervalidasi, maka algoritma kombinasi ini dapat digunakan dalam penyandian pesan dan program yang telah dibuat dapat digunakan sebagai implementasi. Dengan ditingkatkannya algoritma RSA dan digabungkan dengan algoritma ElGamal, diharapkan dapat mempermudah dalam menyandikan pesan serta menambah kesulitan penyadap dalam memecahkan pesan rahasia.