BAB I

PENDAHULUAN

1.1. Latar Belakang

Salah satu media 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.

Kriptografi berasal dari bahasa Yunani, *crypto* dan *graphia*. Crypto berarti *secret* (rahasia) dan graphia berarti *writing* (tulisan). Menurut terminologinya, kriptografi adalah ilmu dan seni untuk menjaga keamanan pesan ketika pesan dikirim dari suatu tempat ke tempat lain (Ariyus, 2008).

Pada kriptografi terdapat istilah *plaintext*, enkripsi, *ciphertext* dan dekripsi. *Enkripsi* adalah sebuah proses penyandian pesan dari yang bisa dimengerti (*plaintext*) menjadi sebuah kode yang tidak bisa dimengerti (*ciphertext*). Sedangkan proses kebalikannya untuk mengubah *ciphertext* menjadi *plaintext* disebut *dekripsi*. Proses enkripsi dan dekripsi memerlukan suatu algoritma dan kunci tertentu.

Algoritma kriptografi terbagi menjadi dua jenis yaitu algoritma simetris dan algoritma asimetris. Algoritma simetris adalah suatu algoritma yang menggunakan kunci enkripsi sama dengan kunci dekripsi. Algoritma asimetris adalah suatu algoritma yang menggunakan kunci berbeda pada proses enkripsi

dan dekripsi. Algoritma asimetris yang populer saat ini adalah algoritma RSA dan algoritma ElGamal.

Algoritma RSA dibuat oleh tiga orang peneliti dari MIT (*Massachussets Institute of Technology*) yaitu Ron (R)ivest, Adi (S)hamir dan Leonard (A)dleman. Kekuatan algoritma ini 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*. Kekurangan dari algoritma ini yaitu membutuhkan kapasitas yang besar sehingga durasi waktu penyandian pesan menjadi lambat jika dibandingkan dengan algoritma simetris.

Algoritma asimetris lainnya yang populer adalah algoritma ElGamal. Algoritma ini dikembangkan pertama kali oleh Taher ElGamal. Kekuatan algoritma ini adalah pada perhitungan logaritma diskrit pada modulo prima yang besar.

Berdasarkan uraian di atas, diketahui bahwa kedua algoritma tersebut aman. Dalam penelitan ini, penulis tertarik untuk mengkaji penggabungan dua algoritma asimetris tersebut agar diperoleh suatu algoritma baru yang bisa digunakan untuk menyandikan pesan yaitu dengan meningkatkan kecepatan algoritma RSA lalu digabungkan dengan algoritma ElGamal, sehingga penulis mengambil judul **"Penyandian Pesan Menggunakan Kombinasi Algoritma RSA yang Ditingkatkan dan Algoritma ElGamal"**.

1.2. Rumusan Masalah

Berdasarkan latar belakang yang penulis uraikan, maka dirumuskan pokok permasalahan pada penelitian ini yaitu:

1. Bagaimanakah algoritma RSA yang ditingkatkan ?
2. Bagaimanakah kombinasi algoritma RSA yang ditingkatkan dan algoritma ElGamal dalam penyandian pesan ?

3. Bagaimanakah program penyandian pesan yang menggunakan kombinasi algoritma RSA yang ditingkatkan dan algoritma ElGamal ?

1.3. Tujuan

Tujuan penelitian ini antara lain:

1. Meningkatkan kecepatan algoritma RSA.
2. Memperoleh algoritma baru yaitu kombinasi algoritma RSA yang ditingkatkan dan algoritma ElGamal dalam penyandian pesan.
3. Memberikan gambaran mengenai implementasi kombinasi algoritma RSA yang ditingkatkan dan algoritma ElGamal dalam bentuk program yang sederhana.

1.4. Manfaat

Manfaat dari penelitian ini adalah sebagai berikut.

1. Menambah pengetahuan penulis dalam melakukan proses enkripsi dan dekripsi pesan menggunakan kombinasi algoritma RSA yang ditingkatkan dan algoritma ElGamal.
2. Memberikan informasi pengembangan algoritma penyandian pesan yang menggabungkan dua algoritma asimetris.
3. Penelitian ini diharapkan dapat memperkenalkan algoritma penyandian pesan yang tetap aman.
4. Sebagai bahan referensi bagi peneliti lain yang ingin membahas topik yang terkait dengan penelitian ini.

1.5. Sistematika Penulisan

Tulisan ini terdiri atas lima bab, yaitu:

1. BAB I PENDAHULUAN

   Bab ini menjelaskan mengenai latar belakang, rumusan masalah, tujuan, manfaat dan sistematika penulisan.

2. BAB II LANDASAN TEORI

   Bab ini membahas teori-teori dasar dan konsep yang berhubungan dan mendukung penulisan skripsi ini. Teori-teori dasar dan konsep tersebut terdiri atas algoritma kriptografi, keterbagian, kekongruenan, grup, gelanggang, sistem ASCII dan Netbeans 8.2.

3. BAB III METODOLOGI PENELITIAN

   Bab ini menjelasakan desain penelitian yang direncanakan dari perumusan masalah, mengkaji model dasar, mengembangkan model dasar, mengkonstruksi program, validasi hingga kesimpulan.

4. BAB IV PEMBAHASAN

   Bab ini memuat hasil penelitian mengenai penyandian pesan yang berdasarkan algoritma RSA yang ditingkatkan dan algoritma ElGamal. Pada bab ini, dijelaskan mengenai algoritma RSA yang ditingkatkan, algoritma kombinasi berdasarkan algoritma RSA yang ditingkatkan dengan Algoritma ElGamal, dan program aplikasi dari algoritma kombinasi tersebut.

5. BAB V KESIMPULAN DAN SARAN

   Bab ini memuat kesimpulan isi keseluruhan uraian bab-bab sebelumnya dan saran-saran dari hasil penulisan skripsi ini.