BAB I

PENDAHULUAN

1.1. Latar Belakang

Kriptografi adalah sebuah seni untuk memanipulasi suatu pesan rahasia ke dalam bentuk yang tidak diketahui oleh banyak orang dengan tujuan pesan rahasia tersebut terlindungi dari orang yang tidak berhak mengetahuinya. Kriptografi mulai digunakan pada abad ke-20 oleh pemerintah untuk kepentingan militer dalam menyampaikan pesan kepada sekutu maupun membobol pesan musuh. Pada perang dunia kedua, pemerintah Nazi Jerman membuat sebuah mesin enkripsi yang dinamakan Enigma. Mesin ini menggunakan beberapa roda berputar untuk melakukan enkripsi dengan cara yang sangat rumit. Tetapi Enigma berhasil dipecahkan oleh pihak sekutu sehingga dapat dikatakan bahwa terpecahkannya mesin ini adalah faktor yang menyebabkan perang dunia kedua tidak lama.

Konsep dasar kriptografi berlandaskan pada teori-teori yang ada dalam ilmu matematika, seperti penguraian bilangan yang sangat besar, komputasi logaritma diskrit, teknik-teknik yang bersifat probabilistik dan lain sebagainya. Teori-teori inilah yang membuat kriptografi menjadi aman digunakan untuk mengirimkan pesan yang bersifat rahasia.

Seiring berjalannya waktu, kriptografi sudah menjadi objek penelitian yang dilakukan oleh banyak orang, dari menggabungkan beberapa metode kriptografi hingga menciptakan metode kriptografi yang baru. Salah satu cara untuk membuat sebuah kriptografi lebih aman adalah dengan menggabungkan dua buah kriptografi, biasa juga disebut dengan algoritma *hybrid* atau kriptografi *hybrid*. Penggabungan dua buah kriptografi akan memiliki banyak keuntungan, terlebih lagi jika metode kriptografi yang digunakan adalah kriptografi yang sulit untuk dipecahkan.

Kriptografi simetri adalah kriptografi yang menggunakan satu buah kunci untuk mengenkripsi dan mendekripsi. Sedangkan kriptografi asimetri adalah kriptografi yang menggunakan dua buah kunci berbeda untuk mengenkripsi dan

mendekripsi. Kriptografi *One Time Pad* merupakan kriptografi simetri yang menggunakan satu buah kunci, ditemukan oleh Major Joseph Mauborgne pada tahun 1917. Kunci kriptografi *One Time Pad* merupakan barisan acak yang dibangkitkan, sehingga ketika digabungkan dengan *plaintext* yang tidak acak maka

akan menghasilkan *ciphertext* dengan barisan yang sepenuhnya acak. Sedangkan kriptografi RSA merupakan kriptografi asimetri yang menggunakan dua buah kunci. Kriptografi ini dibuat oleh Ron Rivest, Adi Shamir, dan Leonard Adleman pada tahun 1976. Kunci kriptografi RSA dibangkitkan dengan menggunakan dua buah bilangan prima, semakin besar bilangan prima yang digunakan maka akan semakin sulit pula kriptografi ini untuk dipecahkan.

Oleh karena itu, dalam penelitian ini akan dilakukan pengembangan kriptografi RSA dan kriptografi *One Time Pad* dengan menggabungkan kedua kriptografi tersebut, dan untuk memudahkan proses perhitungannya maka digunakan program aplikasi java.

1.2. Rumusan Masalah

Berdasarkan latar belakang masalah di atas, maka dapat disusun rumusan masalah sebagai berikut:

1. Bagaimana pengembangan kriptografi RSA dan kriptografi *One Time Pad* dengan menggabungkan kedua kriptografi tersebut?
2. Bagaimana mengonstruksi program aplikasi untuk mempermudah proses dari pengembangan kriptografi RSA dan kriptografi *One Time Pad*?

1.3. Tujuan Penelitian

Berdasarkan rumusan masalah di atas, tujuan dari skripsi ini adalah sebagai berikut:

1. Mengembangkan kriptografi RSA dan kriptografi *One Time Pad* dengan menggabungkan kedua kriptografi tersebut.
2. Mengonstruksi program aplikasi untuk mempermudah proses dari pengembangan kriptografi RSA dan kriptografi *One Time Pad*.

1.4. Batasan Masalah

Berdasarkan latar belakang yang telah diuraikan diatas, maka perlu dibatasi permasalahan dari skripsi ini. Karakter ASCII untuk kunci *One Time Pad* yang digunakan dimulai dari karakter ke-32 sampai dengan karakter ke-126 karena

karakter-karakter tersebut adalah karakter yang umum digunakan dalam suatu penulisan.

1.5. Manfaat Penelitian

Manfaat dari penulisan skripsi ini diharapkan dapat memberikan pengetahuan tentang pengembangan kriptografi RSA dan kriptografi *One Time Pad* dengan menggabungkan kedua kriptografi tersebut yang nantinya dapat dikembangkan lebih lanjut agar dapat memperoleh keamanan yang lebih. Selain itu, untuk mempermudah perhitungan dari algoritma tersebut dibuat juga program aplikasi untuk mengenkripsi dan mendekripsi pesan.

1.6. Sistematika Penelitian

1. BAB I PENDAHULUAN

   Menjelaskan latar belakang masalah, rumusan masalah, tujuan penelitian, manfaat penelitian dan sistematika penelitian.

2. BAB II KAJIAN PUSTAKA

   Menjelaskan kriptografi secara umum, kriptografi RSA, kriptografi *One Time Pad*, teori-teori lain yang mendukung pada BAB IV.

3. BAB III METODOLOGI PENELITIAN

   Menjelaskan perancangan pengembangan kriptografi RSA dan kriptografi *One Time Pad* dengan menggabungkan kedua kriptografi tersebut.

4. BAB IV ALGORITMA HYBRID KRIPTOGRAFI RSA DENGAN KRIPTOGRAFI *ONE TIME PAD*

   Menjelaskan temuan dan bahasan tentang algoritma hybrid kriptografi RSA dengan kriptografi *One Time Pad* yang didapatkan lengkap beserta simulasi kasus.

5. BAB V KESIMPULAN DAN REKOMENDASI

Menjelaskan kesimpulan yang didapat dari penelitian skripsi ini dan rekomendasi yang dapat diaplikasikan oleh pembaca.