BAB III

METODOLOGI PENELITIAN

Adapun tahapan-tahapan yang dilakukan dalam penelitian ini adalah sebagai berikut:

3.1. Masalah Keamanan Kriptografi

Kriptografi telah ada sejak zaman romawi kuno dan berkembang pesat pada abad ke-20 tepatnya pada perang dunia kedua. Pada masa itu kriptografi digunakan untuk mengirimkan sebuah pesan rahasia yang isinya adalah perintah penyerangan. Pembuatan pesan rahasia tersebut dilakukan oleh sebuah mesin yang dinamakan mesin enigma. Pada masa itu mesin ini dianggap mesin yang paling kuat karena tidak dapat dipecahkan oleh siapapun, namun mesin enigma tersebut dapat dipecahkan oleh seorang kriptografer terbaik. Dia telah memecahkan teka-teki yang ada pada mesin enigma tersebut dan membuat perang dunia kedua lebih cepat berakhir.

Seiring dengan berjalannya waktu, kriptografi semakin berkembang. Banyak algoritma kriptografi bermunculan dan banyak pula kriptanalis yang berhasil memecahkan algoritma yang sudah ada. Salah satu cara untuk lebih mempersulit kriptanalis adalah dengan menggabungkan dua algoritma kriptografi agar para kriptanalis tidak dapat memecahkan pesan rahasia yang dikirimkan.

Penggabungan dua algoritma kriptografi disebut juga dengan algoritma hybrid. Algoritma hybrid ini merupakan algoritma yang menggabungkan kriptografi simetri dan kriptografi asimetri. Langkah dari algoritma ini sederhana saja, algoritma dari kunci kriptografi simetri digunakan untuk mengenkripsi *plaintext* dan algoritma dari kunci kriptografi asimetri digunakan untuk mengenkripsi kunci dari kriptografi simetri, sama halnya dengan cara mendekripsinya.

3.2. Kriptografi RSA dan Kriptografi *One Time Pad*

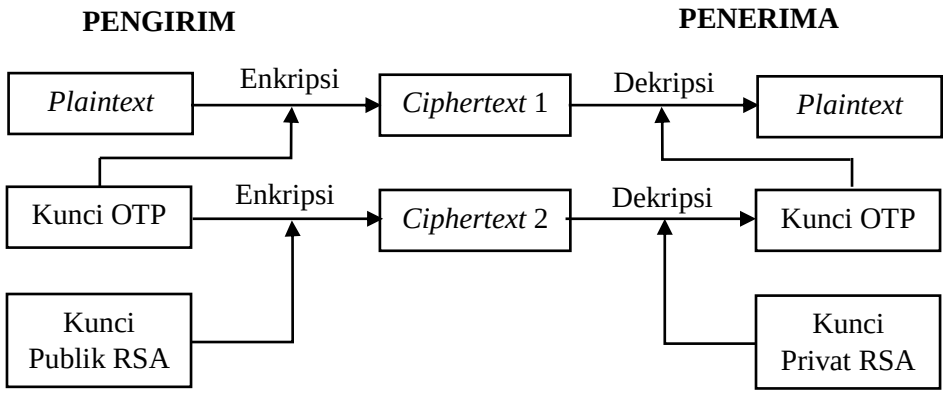
Kriptografi RSA merupakan kriptografi asimetri, keamanan kriptografi RSA terletak pada sulitnya memfaktorkan dua buah bilangan prima yang dimiliki. Terlebih lagi jika dua bilangan prima yang digunakan mencapai 200 digit banyaknya, menurut pencipta kriptografi RSA yaitu Rivest, Shamir dan Adleman

itu akan memakan waktu hingga empat miliar tahun lamanya dengan asumsi menggunakan komputer yang paling canggih pada zaman sekarang. Oleh karena itu, belum ada yang dapat memecahkan kriptografi ini.

Lain halnya dengan kriptografi *One Time Pad*, kriptografi ini ditemukan oleh Major Joseph Mauborgne pada tahun 1917. Kriptografi ini merupakan kriptografi simetri, dan keamanan dari kriptografi ini terletak pada kunci yang dibangkitkan merupakan barisan yang acak, sehingga ketika mengenkripsi *plaintext* yang tidak acak dengan kunci *One Time Pad* yang acak maka akan menghasilkan *ciphertext* yang acak. Oleh karena itu, belum ada yang bisa memecahkan kriptografi ini dan kriptografi ini disebut dengan *unbreakable cipher*.

3.3. Pengembangan Kriptografi RSA dan Kriptografi *One Time Pad*

Pengembangan kriptografi RSA dan kriptografi *One Time Pad* dilakukan dengan cara menggabungkan kedua kriptografi tersebut dengan skema sebagai berikut:



Gambar 3.1. Skema Pengembangan Kriptografi RSA dan Kriptografi *One Time Pad* dengan menggabungkan kedua kriptografi tersebut

Langkah pertama yang dilakukan adalah membangkitkan kunci kriptografi RSA oleh penerima dan mengirimkan kunci publik tersebut kepada pengirim. Proses enkripsi diawali dengan pembangkitan kunci *One Time Pad* yang dibangkitkan secara acak, kemudian kunci tersebut digunakan untuk mengenkripsi *plaintext* yang akan dikirimkan kepada penerima dan menghasilkan *ciphertext* 1.

Setelah itu kunci *One Time Pad* dienkripsi oleh kunci publik RSA yang sudah diterima oleh pengirim dari penerima, dan akhirnya menghasilkan *ciphertext* 2. Kemudian kedua *ciphertext* tersebut dikirimkan kepada penerima untuk selanjutnya didekripsi oleh penerima.

Proses dekripsi diawali dengan mendekripsi *ciphertext* 2 menggunakan kunci privat RSA yang telah dibangkitkan. Dari dekripsi tersebut didapat kunci *One Time Pad* yang kemudian digunakan untuk mendekripsi *ciphertext* 1 sehingga didapat *plaintext* yang dikirimkan oleh pengirim.

3.4. Konstruksi Program Aplikasi

Program aplikasi ini dikonstruksi menggunakan *software* Java, karena *software* ini dapat menampung banyak digit bilangan. Terdapat dua program aplikasi yang dikonstruksi, program aplikasi pertama untuk tampilan pengguna yang terdapat tiga pilihan, yaitu pembangkitan kunci RSA, enkripsi dan dekripsi. Program aplikasi kedua berguna untuk memvalidasi apakah *plaintext* yang telah diterima sama dengan *plaintext* yang asli atau tidak.

3.5. Validasi

Validasi dilakukan untuk mengetahui apakah *plaintext* yang telah diterima sama dengan *plaintext* aslinya atau tidak.

3.6. Kesimpulan

Hasil dari penggabungan dua kriptografi ini adalah algoritma yang lebih banyak untuk dipecahkan, karena ada dua *ciphertext* yang harus dipecahkan untuk menemukan pesan rahasia yang dikirimkan. Kedua kriptografi yang digunakan adalah kriptografi yang terkenal dengan tingkat kerumitan yang tinggi untuk dipecahkan.