BAB V

KESIMPULAN DAN REKOMENDASI

5.1. Kesimpulan

Berdasarkan penelitian ini, dapat diketahui bahwa kesimpulan yang didapat dari penelitian pengembangan kriptografi RSA dan kriptografi *One Time Pad* dengan menggabungkan kedua kriptografi tersebut adalah sebagai berikut:

1. Algoritma ini memiliki tiga tahapan. Tahap pertama adalah pembangkitan kunci RSA oleh penerima yang kemudian kunci publiknya diberikan kepada pengirim. Tahap kedua adalah proses enkripsi pesan oleh pengirim agar pesan yang akan dikirimkan tidak diketahui oleh kriptanalis yang ingin mengetahui pesan tersebut. Tahap terakhir adalah proses dekripsi pesan oleh penerima untuk memperoleh pesan asli yang dikirimkan oleh pengirim. Dengan algoritma ini, kelemahan dari kriptografi *One Time Pad* dapat tertutup oleh kriptografi RSA.
2. Program aplikasi dibuat menggunakan *software* Java. Program aplikasi tersebut bertujuan untuk memudahkan perhitungan algoritma hybrid kriptografi RSA dengan kriptografi *One Time Pad*. Terdapat dua program aplikasi, program aplikasi pertama untuk tampilan pengguna dan program aplikasi kedua untuk validasi program aplikasi pertama, program aplikasi tersebut guna mengetahui apakah pesan asli sama dengan pesan hasil dekripsi atau tidak.

5.2. Rekomendasi

Adapun rekomendasi untuk penelitian ini yaitu sebagai berikut:

1. Karena masih terdapat kelemahan pada algoritma hybrid ini yang telah dijelaskan pada subbab 4.7 bagi peneliti yang akan meneliti pada permasalahan yang sejenis, diharapkan dapat menguji coba setiap serangan pada algoritma hybrid ini dan dapat mengembangkan algoritma hybrid ini menjadi lebih sulit lagi untuk dipecahkan.

2. Selain itu, peneliti juga dapat membuat algoritma hybrid yang lain dengan menggabungkan dua atau lebih kriptografi lain untuk mendapatkan keuntungan-keuntungan dari kriptografi yang digabungkan.
3. Program aplikasi yang dibuat masih belum sempurna, bagi peneliti yang akan mengembangkan program aplikasi tersebut dapat mengembangkan dengan menambahkan bagian untuk membangkitkan bilangan prima secara acak dan bilangan yang relatif prima sehingga pengguna tidak perlu susah mencari bilangan yang akan digunakan. Selain itu, program aplikasi ini juga masih ada kekurangan yaitu jika bilangan prima yang digunakan kurang dari sebelas maka program tersebut akan mengalami *error*.