

BAB V

KESIMPULAN DAN SARAN

Pada bab ini akan dibahas mengenai kesimpulan serta saran mengenai hasil implementasi algoritma OTP CLCG dan RSA-CRT pada pengamanan *coding file*.

5.1 Kesimpulan

Berdasarkan uraian yang telah dijelaskan pada penelitian ini, terdapat beberapa kesimpulan sebagai berikut:

1. Masalah keamanan dalam pertukaran *coding file* dapat dilakukan dengan menggunakan kriptografi OTP CLCG dan RSA-CRT. Pesan dienkripsi dengan menggunakan kunci OTP CLCG dan publik RSA menghasilkan *file* tersamar. Enkripsi dilakukan dengan terlebih dahulu menggunakan algoritma OTP CLCG, lalu dilanjutkan dengan RSA. Sedangkan untuk mengembalikan isi *coding file*, dilakukan melalui proses dekripsi terhadap *file* terenkripsi menggunakan kunci OTP CLCG dan privat RSA-CRT. Dekripsi dilakukan dengan terlebih dahulu menggunakan algoritma RSA-CRT, lalu dilanjutkan dengan OTP CLCG.
2. Program aplikasi dibuat dengan menggunakan bahasa pemrograman *Python*. Aplikasi dibuat dengan menggunakan beberapa library *Python* yaitu *math* untuk operasi matematika dan *Tkinter* untuk membuat tampilan antarmuka. Aplikasi Kriptografi *Coding File* OTP-CLCG RSA-CRT terdiri dari empat menu yaitu menu pembangkitan kunci RSA-CRT, enkripsi, dekripsi dan petunjuk penggunaan aplikasi. Menu pembangkitan kunci RSA-CRT digunakan untuk memperoleh sepasang kunci publik RSA dan privat RSA-CRT. Menu enkripsi digunakan untuk mengamankan *coding file* dengan menggunakan kunci OTP CLCG dan publik RSA. Menu dekripsi digunakan untuk mengembalikan isi *file* memasukkan kunci OTP CLCG dan privat RSA-CRT. Sedangkan menu petunjuk penggunaan diberikan untuk petunjuk bagi pengguna aplikasi.

5.2 Saran

Berdasarkan penelitian yang telah dijalankan, yaitu diharapkan penelitian berikutnya dapat dilakukan untuk jenis *coding file* lainnya.