BAB V

KESIMPULAN DAN SARAN

V.1. Kesimpulan

Setelah dilakukan pengujian dan evaluasi terhadap aplikasi, maka dapat ditarik kesimpulan bahwa :

1. Penerapan algoritma kriptografi elgamal pada program yang telah dibuat adalah sesuai dengan proses algoritma kriptografi elgamal yang ada. Hal ini dibuktikan dengan terbentuknya pasangan kunci publik dan kunci privat.
2. Kunci publik yang dihasilkan terdiri dari tiga buah bilangan yaitu nilai p,g dan y dan kunci privat hanya satu yaitu nilai x.
3. Hasil enkripsi yang dihasilkan memiliki panjang dua kali lipat dari panjang *plaintext* awal. Hal ini dikarenakan setiap blok *plaintext* dienkripsi dengan mencari pasangan *chipertext* $a = g^k \bmod p$ dan $b = y^k m \bmod p$. Sehingga menghasilkan pasangan (a,b).
4. Algoritma kriptografi elgamal dapat diterapkan pada bahasa pemrogram java untuk pengamanan pesan.

V.2. Saran

Saran-saran yang berguna untuk pengembangan lebih lanjut terhadap program aplikasi ini adalah sebagai berikut :

1. Perlu dilakukan pengembangan atau perbaikan pada desain *interface* agar lebih memudahkan pengguna dalam menggukan aplikasi ini.
2. Jenis *file* yang dapat diekripsi hendaknya bukan hanya *file* teks saja tetapi mencakup beberapa *file* seperti *file* gambar, video atau suara.
3. Perlunya dilakukan kombinasi dari dua atau lebih algoritma kriptografi agar lebih menjamin tingat keamanan data.