BAB V
PENUTUP

5.1 Kesimpulan

Berdasarkan pembahasan dari penelitian yang dilakukan pada perancangan aplikasi kriptografi file citra medis dengan menggunakan algoritma AES dan algoritma ElGamal, dapat ditarik kesimpulan sebagai berikut :

a. File citra medis dapat diamankan menggunakan algoritma AES. Hasil enkripsi file citra medis menggunakan algoritma AES, menghasilkan file citra baru yang tidak dapat diketahui artinya sebelum didekripsi kembali sehingga algoritma ini berhasil mengamankan file citra medis tersebut.
b. Algoritma ElGamal dapat meningkatkan keamanan pada kunci AES. Hal ini dapat terjadi karena pengirim menjadi tidak terlalu khawatir untuk mengirimkan kunci AES yang telah dienkripsi melalui jalur publik kepada penerima. Selain itu, konsep algoritma asimetri pada algortima ElGamal juga dapat meningkatkan keamanan pada pengamanan kunci AES.
c. Algoritma AES dapat digunakan untuk mendekripsi file citra medis. Hasil dari citra yang didekripsi sama dengan citra asli, hal ini diperkuat dengan perbandingan nilai *checksum* pada file citra asli dan file hasil dekripsi yang tidak ditemukan perbedaan.
d. Proses dekripsi menggunakan kombinasi Algoritma AES dan Algoritma ElGamal lebih cepat dibandingkan dengan proses enkripsi.

5.2 Saran

Saran yang bisa dilakukan untuk penelitian lanjutan dari penelitian ini adalah :

a. Menggunakan ekstensi file citra yang lebih luas, tidak hanya terbatas pada file dengan format BMP.
b. Melakukan analisis yang lebih mendalam pada kelebihan dan kekurangan penggunaan setiap mode operasi pada file citra medis.

c. Melakukan analisis kombinasi antara algoritma AES dengan algoritma lainnya untuk mengetahui perbandingan efisiensi pada proses enkripsi maupun dekripsi.