BAB V

KESIMPULAN DAN SARAN

V.1. Kesimpulan

Berikut adalah kesimpulan dari hasil kegiatan penelitian yang telah dilakukan :.

1. Algoritma *AES* merupakan algoritma yang sulit dipecahkan, karena algoritma *AES* 128 bit memiliki ruang kunci 2^{128} yang merupakan nilai yang sangat besar dan dianggap aman untuk digunakan sehingga terhindar dari *brute force attack.*
2. Pada proses enkripsi *AES* mengunakan 4 transformasi dasar dengan urutan trasformasi *subbytes, shiftrows, mixcolumns,* dan *addroundkey.* Sedangkan pada proses *dekripsi* mengunakan *invers* semua transformasi dasar pada algoritma *AES* kecuali *addroundkey* dengan urutan transformasi *invshiftrows, invsubbytes, addroundkey*,dan *invmixcolumns.*
3. Proses yang dibutuhkan untuk melakukan enkripsi terhadap sebuah *file* gambar memakan waktu yang relatif lama, tergantung dengan ukuran atau besar *file* dan kunci yang dipergunakan.

V.2. Saran

Berikut adalah merupakan saran untuk mengembangan aplikasi :

1. Perlu dilakukan ditambahkan fungsi login dan penggunaan *database* sehingga aplikasi tidak dipergunakan oleh pihak yang tidak berkepentingan.
2. Sebaiknya ditambahkan fungsi agar pengguna dapat memilih jenis algortima yang akan dipergunakan seperti 128 bit, 192 bit dan 256 bit.