BAB V

PENUTUP

5.1. Kesimpulan

Berdasarkan hasil analisis dan implementasi yang telah dilakukan, serta untuk mengakhiri penelitian pada laporan skripsi yang berjudul "**Aplikasi Dekripsi dan Enkripsi Pesan dengan Algoritma Data Encryption Standard (DES) berbasis Java**" maka penulis dapat menarik kesimpulan sebagai berikut :

1. Alur Algoritma *Data Encryption Standard (DES)* dilakukan dengan cara merubah *plaintext* dan *key* kedalam bentuk biner yang kemudian akan dibagi kedalam blok-blok biner sesuai ketentuan dari algoritma DES. Pesan atau *plaintext* yang digunakan berukuran 64 bit dan kunci yang digunakan berukuran 64 bit. Setelah *plaintext* dirubah menjadi biner, maka akan dilakukan permutasi awal menggunakan tabel *Initial Permutation*, lalu hasil dari permutasi ini dibagi menjadi 2 blok biner, yakni R0 dan L0. Langkah selanjutnya, *key* yang sudah berbentuk biner, dilakukan operasi untuk membangkitkan 16 buah anak kunci yang nantinya akan digunakan untuk mengenkripsi pesan. Setelah didapat 16 buah anak kunci tersebut, kemudian dimulailah perputaran 16 kali DES. Setelah perputaran selesai, tahap terakhir adalah melakukan permutasi R16L16 menggunakan tabel IP Invers. Perbedaan mendasar antara enkripsi dan dekripsi menggunakan algoritma DES adalah pada penggunaan 16 buah anak kunci. Pada proses enkripsi, kunci yang

digunakan untuk perputaran adalah K1 sampai K16, sedangkan untuk dekripsi, kunci yang digunakan dimulai dari K16 sampai dengan K1.

2. Pada aplikasi ini, proses enkripsi dan dekripsi dapat dilakukan secara bertahap. Penulis membagi langkah-langkah enkripsi dan dekripsi menjadi 6 langkah. Yang pertama, adalah melakukan konversi nilai masukan *plaintext* dan *key* kedalam biner, kemudian melakukan Initial Permutation. Langkah ketiga adalah pembangkitan kunci dengan diawali pencarian K+, baru kemudian dilangkah keempat akan ditemukan hasil dari pembangkitan 16 anak kunci tersebut. Langkah kelima adalah melakukan putaran 16 kali sesuai aturan algoritma DES. Langkah keenam atau terakhir adalah melakukan permutasi menggunakan tabel IP Invers.
3. Aplikasi ini sudah dirancang sedemikian rupa agar dapat mengenkripsi dan mendekripsi pesan tanpa harus melalui langkah-langkah panjang. Jadi, proses enkripsi dan dekripsi ini sudah secara otomatis dijalankan oleh komputer tanpa harus menampilkan kepada user bagaimana proses ini berjalan.
4. Algortima DES membatasi panjang karakter sebuah pesan yang akan dienkripsi dan didekripsi. Oleh karena itu, untuk dapat menenkripsi dan mendekripsi pesan berupa kalimat panjang, maka yang harus dilakukan adalah membagi kalimat itu menjadi blok-blok dimana setiap blok berisi 64 bit atau 8 karakter. Lalu, apabila ada blok yang belum terisi 64

bit atau 8 karater, maka akan diganti dengan karakter spasi sehingga bisa memenuhi ketentuan 64 bit algoritma DES.

5.2. Saran

Dalam penulisan skripsi ini tentu masih terdapat banyak kekurangan, namun ini tidak menutup untuk dapat disempurnakan untuk pengembangan selanjutnya agar dapat meningkatkan fungsionalitasnya dan manfaat aplikasi ini. Beberapa hal yang mungkin dapat dilakukan untuk pengembangan aplikasi Encrypt Decrypt DES ini yaitu:

1. Merubah metode konversi ke biner yang masih menggunakan Array menjadi bertipe Byte.
2. Menambah logika untuk menyaring masukan berupa Hexadecimal dan Biner agar lebih akurat.
3. Mengganti tutorial statis menjadi dinamis, seperti flash atau gambar bergerak agar menarik dan tidak membosankan.
4. Memperbaiki *Graphical User Interface (GUI)* agar kelihatan lebih bagus dan lebih *user friendly*.
5. Menambah algoritma kriptografi lain supaya bervariasi dan bisa digunakan untuk metode kriptografi *hybrid*.
6. Menambahkan menu *Help* atau menu bantuan agar aplikasi ini bisa digunakan oleh orang awam.