BAB V

KESIMPULAN DAN SARAN

5.1 Kesimpulan

Kesimpulan dari penelitian modifikasi algoritma DES 64-bit dengan pengujian *avalanche effetcs* dan *randomness test* untuk pengamanan pada penyimpanan *file* adalah sebagai berikut :

1. Modifikasi bagian *S-Box* dengan meng-*xor*-kan nilai tiap kunci dan di mod 16 hasil *xor* kunci merupakan langkah untuk membuat acak nilai elemen *S-Box*, begitu juga dengan *P-Box*. Hanya saja modulus untuk *P-Box* adalah 32 sehingga akan menyulitkan kriptanalis.
2. Hasil pengujian DES 64 bit dengan modifikasi *S-Box* dan *P-Box* berpengaruh terhadap waktu proses enkripsi dan dekripsi pada masukkan *file* dengan ukuran lebih dari 3 MB. Dari segi efisiensi, DES 64 bit baik untuk penyimpanan *file* dengan berbagai ekstensi karena *file* hasil enkripsi sama dengan *file* asli, terlebih jika ditambah dengan fungsi kompresi maka ukuran *file* hasil enkripsi akan lebih kecil dari ukuran *file* aslinya.
3. Modifikasi *S-Box* dan *P-Box* menjadi lebih dinamis (tergantung pada masukkan kunci) membuat rata-rata nilai *avalanche effects* 50% dan lolos uji *randomness test* sehingga DES 64 bit dengan modifikasi ini baik untuk diimplementasikan pada sistem yang lain, namun pada modifikasi *S-Box_P-Box* dengan kunci 10101010 nilai *avalanche effect*-nya 40.625% dan kurang baik jika diimplementasikan.

5.2 Saran

Saran dari penelitian modifikasi algoritma DES 64-bit ini adalah sebagai berikut :

1. Modifikasi *S-Box_P-Box* dengan kunci 10101010 mendapatkan nilai *avalanche effects* yang kurang baik sehingga penelitian selanjutnya diharapakan bisa lebih baik lagi dengan memodifikasi bagian DES 64 bit yang masih statik seperti
   - permutasi ekspansi,
   - permutasi kompresi (PC-1) dan
   - permutasi kompresi (PC-2)
2. Tingkatkan kompleksitas kombinasi kunci untuk membuat *ciphertext* lebih acak.
3. Gunakan kompresi berbasis dictionary agar *file* hasil enkripsi bisa lebih kecil dari *file* asli setelah dienkripsi dan *file* hasil dekripsi sama dengan *file* asli.