BAB V
KESIMPULAN DAN SARAN

5.1 Kesimpulan

1. Telah diimplementasikan sebuah perangkat lunak yang menggunakan algoritma kriptografi *CAST-128* kemudian dari uji waktu proses algoritma *CAST-128,* diperoleh kesimpulan bahwa waktu proses enkripsi untuk ukuran *file* 50KB rata-rata waktu enkripsi adalah sebesar 0,807 detik, untuk ukuran *file* 500KB rata-rata waktu enkripsi adalah sebesar 8,412 detik kemudian rata-rata waktu dekripsi untuk ukuran *file* 50KB adalah sebesar 0,794 detik, untuk ukuran *file* 500KB adalah sebesar 8,451 detik.
2. Dari uji *avalanche effect* dapat disimpulkan bahwa nilai rata-rata perubahan yang menghasilkan nilai *avalanche effect* yang ideal (45% sampai 60%) adalah pada perubahan *key,* dimana pada perubahan *byte* menghasilkan nilai 50,12% dan pada perubahan bit menghasilkan nilai 49,79%.
3. Kemudian untuk nilai rata-rata perubahan yang menghasilkan nilai *avalanche effect* yang kurang ideal adalah pada perubahan *chipertext dan plaintext,* dimana pada perubahan *byte plaintext* menghasilkan nilai 36,15%, pada perubahan bit *plaintext* menghasilkan nilai 36,48%, pada perubahan *byte chipertext* menghasilkan nilai 23,44% dan pada perubahan bit *chipertext* menghasilkan nilai 23,39%.

Dengan nilai *avalanche effect* yang dihasilkan pada pengujian terhadap *key*, dapat disimpulkan bahwa algoritma *CAST-128* cukup tahan terhadap serangan kriptanalisis.

5.2 Saran

Saran yang mungkin bisa jadi bahan pertimbangan adalah pada pengujian *avalanche effect* posisi pengujian bit/*byte* bisa di buat lebih bervariasi lagi. Begitu juga pada jumlah bit/*byte* yang diuji bisa ditambah lagi untuk mendapatkan hasil yang lebih akurat.