BAB V

KESIMPULAN DAN SARAN

5.1 Kesimpulan

Dari analisa yang telah dilakukan pada bab IV, maka dapat ditarik kesimpulan-kesimpulan sebagai berikut :

1. Algoritma kriptografi *Vertical Bit Rotation* (VBR) 32 Bit dapat digunakan dalam mengamankan data berupa *file* yang disimpan secara *online* dan proses enkripsi dan dekripsi terjadi di *server*.

2. Algoritma kriptografi VBR 32 Bit dapat diterapkan menggunakan bahasa pemrograman PHP.

3. Dengan penambahan jumlah *round*, proses *Add Key*, proses *SubBlock Rotation*, proses *Byte Substitution*, proses *Add SubKey*, dan proses *Binary Rotation* dapat meningkatkan nilai *Avalanche Effect* sehingga tingkat keamanan algoritma kriptografi VBR 32 Bit masuk dalam kategori baik.

4. Dengan mengolah data nilai *Avalanche Effect* dari beberapa eksperimen yang dilakukan dapat diambil kesimpulan bahwa algoritma kriptografi VBR 32 Bit sangat baik bila memiliki jumlah *round* lebih besar dari 2 *round*.

5. Dari data hasil uji coba pada sistem operasi 32 bit dan 64 bit, algoritma kriptografi VBR 32 Bit dapat diimplementasikan pada sistem operasi 32 bit dan sistem operasi 64 bit.

5.2 Saran

1. Harus dilakukan pengujian lebih lanjut tentang keamanan algoritma kriptografi VBR 32 Bit dengan parameter selain *avalanche effect*.

2. Perlu pengembangan lebih lanjut bila dirasa perlu pada algoritma kriptografi VBR 32 Bit agar memiliki tingkat keamanan yang lebih baik dengan tanpa menghilangkan prinsip dasar dari algoritma kriptografi VBR yaitu kesederhanaan.