

## BAB V

### KESIMPULAN DAN SARAN

#### V.1. Kesimpulan

Pada tahap ini merupakan hasil dari penelitian yang dirangkum dengan beberapa kesimpulan. Penulis mengambil suatu kesimpulan sebagai berikut:

1. Perangkat lunak yang dibuat dapat melakukan enkripsi *folder* dengan menggabungkan seluruh isi *folder* dalam satu *file* sehingga tidak memungkinkan pengaksesan isi dan struktur *folder* dari Windows Explorer.
2. Jumlah folder yang dikandung dalam suatu folder yang akan dienkripsi mempengaruhi waktu enkripsi itu sendiri. Begitu pula untuk proses dekripsi.
3. Hasil enkripsi *folder* dengan aplikasi yang dibuat selalu memiliki ukuran yang lebih besar daripada ukuran semula. Hal ini disebabkan oleh kebutuhan enkripsi algoritma *Serpent* yang melakukan enkripsi setiap blok berukuran 128 bit (16 byte).
4. Algoritma *serpent* dirancang oleh Ross Anderson, Eli Biham, Lars Knudsen dan merupakan salah satu algoritma yang pernah menjadi finalis dalam kompetisi Advanced Encryption Standar (AES) yang menduduki perangkat ke 2 untuk algoritma *serpent*. Algoritma *serpent* adalah algoritma *chipper block* dengan 32 putaran jaringan *substitution permutation* (SP) yang beroperasi pada empat *word* 32 bit, yang berarti adalah 128 bit.

5. Aplikasi yang penulis rancang dengan aplikasi *Visual Basic 2010* yang dapat memudahkan pengguna (*user*) dalam menjalankan aplikasi hanya bisa mengenkripsi data pada *folder*.

## V.2. Saran

Adapun saran yang penulis kemukakan adalah sebagai berikut:

1. Hasil perancangan hanya mencakup pengamanan data pada *folder* dengan menggunakan satu algoritma yaitu algoritma *serpent* untuk pengembangan lebih lanjut dibutuhkan keamanan dengan penambahan algoritma-algoritma yang berbeda sebagai pilihan untuk pengenkripsian *folder*.
2. Dalam aplikasi ini, algoritma *serpent* hanya mampu mendekripsi *folder* berukuran maksimal 500 KB saja. Diharapkan pengembangan aplikasi ini mampu mendekripsi data dalam *folder* dengan ukuran data yang lebih besar.