BAB V

KESIMPULAN DAN SARAN

5.1 Kesimpulan

Dari penelitian yang dilakukan, dapat disimpulkan bahwa aplikasi pengaman berkas digital yang dapat digunakan untuk enkripsi dan dekripsi berkas digital dengan algoritma kriptografi Twofish telah berhasil dibangun. Dengan menggunakan aplikasi ini, pengguna dapat menjaga kerahasiaan isi dari sebuah berkas dengan tidak dapat diakses oleh pihak tak berwenang tanpa pengetahuan akan *password* yang digunakan.

Berdasarkan hasil uji coba aplikasi, diketahui bahwa performa implementasi algoritma twofish pada aplikasi dapat dikatakan memadai dengan membutuhkan waktu sekitar 1 detik untuk mengenkripsi dan mendekripsi berkas berukuran 1 MB menggunakan *key* berukuran 256 bit. Berkas terenkripsi juga tidak dapat dibuka menggunakan aplikasi yang berkaitan dengan berkas sebelum dienkripsi. Seluruh jenis berkas dapat dienkripsi dan dipulihkan menggunakan *key* yang sesuai. Perubahan pada berkas terenkripsi mengakibatkan kerusakan dan berkas menjadi tidak berguna.

5.2 Saran

Beberapa saran yang diajukan untuk pengembangan lebih lanjut terhadap penelitian ini adalah sebagai berikut:

1. Perbandingan performa algoritma kriptografi twofish dengan menggunakan mode operasi yang berbeda, seperti mode *Output Feedback* (OFB) atau mode *Counter* (CTR).
2. Penggunaan algoritma kompresi berkas seperi algoritma DEFLATE pada aplikasi, sehingga ukuran berkas yang harus dienkripsi menjadi lebih kecil dan mengurangi waktu yang dibutuhkan untuk mengenkripsi berkas.
3. Pengembangan aplikasi *Full Disk Encryption* menggunakan algoritma twofish untuk mengenkripsi *Hard Disk* secara keseluruhan. Dengan pengembangan ini, keamanan seluruh data yang ada pada sebuah komputer terjamin dan pengguna tidak perlu memilih berkas yang ingin dienkripsi. Implementasi ini juga mencegah kelalaian pengguna dalam mengenkripsi seluruh berkas yang sensitif.