BAB V

PENUTUP

5.1 Kesimpulan

Kesimpulan yang dapat diambil dari studi dan implementasi algoritma Twofish pada *CryptTwo* adalah:

1. Algoritma Twofish dapat diimplementasikan ke dalam banyak bahasa pemrograman dan algoritma serta sifat perancangannya terbuka bagi umum. Algoritma Twofish awalnya diimplementasikan ke dalam bahasa C. Kemudian berkembang ke berbagai bahasa pemrograman karena sifatnya yang *open source*. Dalam penelitian ini diimplementasikan ke dalam J2SE menjadi sebuah model kriptosistem berbasis desktop.
2. Implementasi algoritma Twofish yang optimal dapat dilakukan dengan aplikasi yang tidak sering berubah-ubah kunci serta tidak menggunakan *weak-key*. Dalam fungsi F terdapat total 521 iterasi untuk menghasilkan semua subkunci yang dibutuhkan. Aplikasi kemudian dapat menyimpan subkunci ini dan tidak membutuhkan langkah-langkah proses penurunan berulang kali, kecuali kunci yang digunakan berubah. Kunci yang sering berubah akan membutuhkan proses penurunan baru pada iterasi yang panjang, hal ini akan membuat waktu kerja Twofish lebih panjang. Sedangkan penggunaan *weak key* dapat mengganggu hasil enkripsi dan dekripsi. *Weak key* membuat hasil enkripsi/dekripsi menjadi tidak konsisten.

3. Tingkat keamanan algoritma Twofish ditentukan oleh jumlah iterasi dan panjang kunci dan kerahasiaan kunci yang digunakan. Jumlah iterasi yang digunakan dengan semestinya membuat jaringan feistel pada Twofish bekerja secara konsisten (16 iterasi), pengurangan jumlah iterasi akan mengurangi tingkat kekuatan ciphertext. Sedangkan peran panjang dan kerahasiaan kunci menjadi sangat krusial. Kunci yang panjang menjadi sama tingkat kebutuhannya dengan iterasi yang tidak dikurangi. Karena proses pembangkitan *sub key* akan menjadi lebih acak dan membutuhkan waktu lama untuk dipecahkan. Begitu juga dengan kerahasiaan kunci. Jika kunci sudah diketahui oleh pihak yang tidak berkepentingan, maka akan sangat mudah memecahkan *ciphertext* atau *plaintext* tanpa *attack* tertentu sekalipun.

5.2 Saran

Untuk lebih menyempurnakan aplikasi ini, terdapat beberapa saran yang mungkin dapat dipergunakan antara lain :

1. Logika program dapat dikembangkan lagi untuk optimasi kerja sistem. Hal ini agar sistem mampu melakukan enkripsi/dekripsi terhadap lebih banyak tipe masukan data dan kapasitasnya.
2. Kunci pada sistem dapat menjadi sebuah pilihan saja bagi user (bukan masukan). Hal ini menjadi faktor pendukung tingkat kekuatan sistem. Akan lebih baik jika sistem dapat menyediakan fitur pendidstribusian kunci demi menjaga kerahasiaan kunci.

3. Sistem dapat lebih optimal diterapkan pada spesifikasi hardware yang lebih tinggi. Twofish membutuhkan kerja CPU yang besar. Sehingga kinerja Twofish akan lebih baik dalam spesifikasi hardware yang memadai. Dalam hal ini adalah untuk mengenkripsi/dekripsi file dengan ukuran yang lebih besar.
4. Sistem dapat dikembangkan menjadi lebih terstruktur dengan implementasi database terhadapnya. Sehingga user bisa menyimpan dan me*load* kembali hasil kerjanya.
5. Sistem dapat dikembangkan lagi untuk mampu menghasilkan output proses dekripsi file (hingga saat ini output dihasilkan pada textarea sehingga membutuhkan proses manual untuk dapat digunakan kembali) sehingga file dekrip dapat digunakan lagi.