BAB V

PENUTUP

5.1 Kesimpulan

Kesimpulan yang dapat diambil dari studi dan implementasi algoritma Blowfish adalah:

1. Algoritma Blowfish menerapkan jaringan Feistel (*Feistel Network*) yang terdiri dari 16 putaran. Blowfish merupakan cipher blok. Yang berarti selama proses enkripsi dan dekripsi, Blowfish bekerja dengan membagi pesan menjadi blok-blok bit dengan ukuran sama panjang yaitu 64-bit dengan panjang kunci bervariasi yang mengenkripsi data dalam 8 byte blok. Pesan yang bukan merupakan kelipatan 8 byte akan ditambahkan bit-bit tambahan (*padding*) sehingga ukuran untuk tiap blok sama . Algoritma Blowfish terdiri dari dua bagian: key expansion dan enkripsi data.
2. Algoritma Blowfish dapat diimplementasikan ke dalam banyak bahasa pemrograman dan algoritma serta sifat perancangannya terbuka bagi umum. Algoritma Blowfish awalnya diimplementasikan ke dalam bahasa C. Kemudian berkembang ke berbagai bahasa pemrograman karena sifatnya yang *open source*. Dalam penelitian ini diimplementasikan ke dalam Microsoft Visual Basic 6.0 menjadi sebuah model kriptosistem berbasis desktop. File yang dapat di enkripsi dan dekripsi adalah file Microsoft

Office meliputi file Microsoft Word (.doc, .docx, .rtf, .txt), Microsoft Excel (.xls, .xlsx), Microsoft Access (.mdb) dan Microsoft PowerPoint (.ppt, .pptx).

3. Pengujian yang dilakukan adalah pengujian kunci, pengujian berbagai jenis file Microsof Office, pengujian putaran Blowfish dan pengujian tool tambahan yaitu Lock Folder.
   a. Pengujian kunci

      Dalam pengujian kunci, maka bisa dikatakan bahwa kunci yang dipakai untuk uji coba sistem bukanlah kunci yang lemah.

   b. Pengujian berbagai jenis file Microsof Office
      - Semua jenis file Microsoft Office meliputi file Microsoft Word (.doc, .docx, .rtf, .txt), Microsoft Excel (.xls, .xlsx), Microsoft Access (.mdb) dan Microsoft PowerPoint (.ppt, .pptx) dapat dilakukan proses enkripsi dan dekripsi.
      - Hasil enkripsi pada file .doc, .rtf, .txt, dan .xls dapat dibuka, sedangkan hasil enkripsi pada file .docx, .xlsx, .mdb, .ppt, dan .pptx tidak dapat dibuka, tetapi dapat di dekripsi menjadi file semula.

c. Pengujian putaran Blowfish

Implementasi algoritma Blowfish yang optimal dan aman dari pembongkaran pesan, maka algoritmanya harus menggunakan 16 putaran.

d. Pengujian Lock Folder

Tool Lock Folder dapat digunakan untuk mengamankan suatu folder.

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. Sistem dapat dikembangkan menjadi lebih terstruktur dengan implementasi database terhadapnya. Sehingga user bisa menyimpan dan me-*load* kembali hasil kerjanya.
3. Untuk lebih menjamin keamanan enkripsi data/file Blowfish juga dapat dikolaborasikan dengan algoritma-algoritma enkripsi lainnya