

BAB VII

PENUTUP

7.1 Kesimpulan

Dari analisis studi dan aplikasi enkripsi/dekripsi file dengan menggunakan algoritma RC4 dapat disimpulkan bahwa:

1. Waktu proses enkripsi/dekripsi file tergantung pada ukuran file yang akan dienkripsi/dekripsi. Semakin besar ukuran file maka waktu proses enkripsi/dekripsi file semakin lama. Hal ini disebabkan oleh efek cache dan efek penanganan file (*file handling*) oleh sistem operasi. (Dan untuk aplikasi ini sebaiknya batas ukuran file maksimal sebesar 2 MB untuk mempercepat proses enkripsi file).
2. Ukuran file sebelum proses enkripsi dengan ukuran file setelah proses enkripsi tidak mengalami perubahan karena algoritma RC4 tidak melakukan pengompresan file. Untuk mengompresi file diperlukan analisis dan algoritma tersendiri.
3. Dengan menggunakan file yang sama dengan ukuran kunci yang berbeda-beda tidak mempengaruhi kecepatan proses enkripsi. Panjang kunci user hanya memiliki hubungan dengan stream generator sehingga berapapun besar panjang kunci, kecepatan proses enkripsi dan dekripsi tidak terpengaruh.

7.2 Saran

Untuk meningkatkan keamanan data dapat ditambahkan proses pengkompresan file sebelum proses enkripsi, karena kriptanalisis mengandalkan pada redundansi pada plaintext, mengkompresi file sebelum proses enkripsi mengurangi redundansi plaintext.

Selain itu penghapusan data sumber, cara yang lebih aman adalah dengan menulis langsung ke hardisk tanpa melalui disk cache, karena ada kemungkinan data belum dituliskan semua ke-harddisk ketika dihapus (karena masih ada didalam cache).

