BAB VII

SIMPULAN DAN SARAN

7.1. Simpulan

Dari hasil analisis studi dan implementasi algoritma RC6 untuk enkripsi dan dekripsi data dapat diambil beberapa kesimpulan, yaitu :

1. RC6 adalah algoritma enkripsi dengan model *private key*/kunci pribadi yang mempunyai key dekripsi sama dengan key enkripsi..
2. Algoritma RC6 merupakan *block cipher* dengan ukuran *block* hingga128 bit dan parameter yaitu RC6-w/r/b dengan nilai w=32 sebagai ukuran kata dalam bit, r=20 sebagai banyaknya iterasi/*round* dan b ukuran kunci yang bervariasi antara 16, 24 dan 32 *byte.*
3. Algoritma RC6 terdiri dari 3 bagian yaitu *key setup*, *whitening* dan *ciphering.*
4. Waktu proses enkripsi dan deskripsi tergantung pada besarnya *file* yang akan dienkripsi/dekripsi. Hal ini disebabkan oleh efek *cache* dan efek penanganan *file* (*file handling*) oleh sistem operasi.
5. Ukuran *file* pada proses enkripsi/dekripsi mengalami sedikit perubahan, hal ini dikarenakan terjadinya proses *padding.*
6. Dengan menggunakan panjang kunci yang berbeda pada proses enkripsi yang dilakukan pada *file* yang sama, waktu proses tidak mengalami perubahan yang besar. Perubahan yang terlihat disebabkan format waktu proses yang sangat detail.

7. Algoritma RC6 merupakan algoritma enkripsi yang *simple, fast, and secure.*

7.2. Saran

Untuk dapat lebih mengetahui tingkat keamanan algoritma RC6, keefisienan, dan kecepatanya, maka algoritma RC6 harus bisa lebih disebar luaskan agar semakin banyak yang menganalisis algoritma ini sehingga dapat lebih diketahui kelebihan dan kekurangannya.

Adapun untuk perangkat lunak yang telah dihasilkan ini dapat dilakukan pendalaman lebih lanjut, sehingga dalam pengembangannya dapat menghasilkan sebuah perangkat lunak yang lebih baik. Dapat juga algoritma RC6 ini dibuat dengan bahasa pemrograman yang lain, misalnya dalam bentuk web sehingga bisa diketahui perbandingan algoritma RC6 pada pengimplementasian dengan bahasa pemrograman lainnya.

Perangkat lunak yang telah dihasilkan ini dapat dilakukan penelitian lebih lanjut untuk dapat mengetahui kesalahn *logical* program yang terjadi pada proses enkripsi/dekripsi text. Untuk itu sangat disarankan, dalam penggunaan perangkat lunak yang dihasilkan terutama pada proses enkripsi/dekripsi text sebaiknya dilakukan minimal dua kali untuk mengetahui apakah hasil enkripsi/dekripsi telah sesuai dengan hasil yang diharapkan. Penggunaan perangkat lunak ini kami sarankan untuk lebih memprioritaskan pemanfaatannya pada proses enkripsi/dekripsi file.

Dalam pengembangan lebih lanjut perangkat lunak ini, disarankan agar lebih memperhatikan dalam aspek penggunaan bahasa yang lebih baik.