BAB V

PENUTUP

5.1 Kesimpulan

Dari keseluruhan bab pada skripsi ini, maka dapat diambil kesimpulan sebagai berikut :

1. Pada proses enkripsi/dekripsi menggunakan algoritma RSA dan digital signature menggunakan kunci publik dan kunci private, file hasil enkripsi bertambah besar karena adanya penambahan bit-bit kunci dan kode-kode enkripsi. Adanya perbedaan kode hasil proses enkripsi baik inputan secara manual melalui keyboard ataupun inputan file teks yang sudah ada. Setiap kali proses enkripsi teks dilakukan, maka akan menghasilkan kode yang berbeda-beda, walaupun *plaintext* yang dimasukkan sama.
2. Pada proses enkripsi/dekripsi file non-teks, ukuran file hasil enkripsi bertambah, karena adanya penambahan dua *array bytes* terpisah yang digunakan dalam proses enkripsi, yaitu *kunci* dan *kunciIV*, yang digunakan untuk menghindari seseorang melakukan rekayasa balik agar mendapatkan kunci dan untuk mengenkrip blok pertama data.
3. *Digital signature* diberikan pada teks yang telah dienkripsi berupa bit-bit yang berfungsi untuk menjaga keabsahan data. *Digital signature* memanfaatkan fungsi *hashing MD5CryptoServiceProvider*.
4. *Tool File Shredder* dapat menghancurkan file dengan baik dan waktu yang dibutuhkan untuk menghancurkan masing-masing file tergantung kepada

ukuran file itu sendiri dan kekuatan penghancuran yang dipilih. Semakin besar ukuran file, maka waktu yang dibutuhkan untuk menghancurkan file akan semakin lama.

5.2 Saran

Perangkat lunak ini masih masih dapat dikembangkan lagi agar menjadi model yang lebih baik lagi. Beberapa saran untuk pengembangan dari perangkat lunak ini adalah sebagai berikut :

1. Sangat memungkinkan untuk melakukan sebuah penelitian lanjutan mengenai penerapan algoritma RSA untuk pengamanan data dan digital signature, dimana penelitian ini sangat ditunjang oleh sumber yang memadai baik dari ide logika dan algoritmanya dan lingkungan penelitian yang dibutuhkan.
2. Model ini dapat dikembangkan lagi dengan menggunakan source yang tidak terlalu besar namun mempunyai kelebihan yang berlimpah.
3. Model ini dapat dikembangkan menjadi lebih terstruktur dengan implementasi database di dalamnya. Sehingga bisa menyimpan *event log*, yaitu informasi aktifitas apa saja yang telah dilakukan.