



Hak cipta dan penggunaan kembali:

Lisensi ini mengizinkan setiap orang untuk menggubah, memperbaiki, dan membuat ciptaan turunan bukan untuk kepentingan komersial, selama anda mencantumkan nama penulis dan melisensikan ciptaan turunan dengan syarat yang serupa dengan ciptaan asli.

Copyright and reuse:

This license lets you remix, tweak, and build upon work non-commercially, as long as you credit the origin creator and license it on your new creations under the identical terms.

BAB V

KESIMPULAN DAN SARAN

5.1 Kesimpulan

Berdasarkan hasil uji penelitian yang sudah dilakukan, maka dapat ditarik kesimpulan sebagai berikut.

1. Aplikasi pembelajaran untuk memahami pengamanan file dengan menggabungkan metode SHA256, *Rivest-Shamir-Adleman* (RSA) dan *Twofish* telah berhasil dibangun dan berjalan sesuai dengan rancangan.
2. Nilai dari hasil rata – rata *throughput* dari ketiga proses kurang optimal, tetapi nilai hasil rata – rata *throughput* proses hashing masih lebih tinggi dibanding nilai hasil rata – rata *throughput* proses enkripsi dekripsi RSA dan *twofish*. Nilai hasil rata – rata *throughput* yang tidak optimal dapat disebabkan oleh adanya pengaruh *memory leak* dan *memory fragmentation* yang tidak ditangani dengan baik.
3. Hasil waktu rata – rata proses *hashing* SHA256 lebih besar dibanding waktu rata - rata proses enkripsi dekripsi dari algoritma RSA dan *twofish*. Perbedaan ini disebabkan karena ukuran file yang digunakan pada proses *hashing* bervariasi, sedangkan ukuran file yang pada proses enkripsi dekripsi RSA dan *twofish* tidak berubah.

5.2 Saran

Berdasarkan penelitian yang telah dilakukan, berikut adalah saran yang dapat digunakan untuk kepentingan penelitian berikutnya.

1. Perbandingan *throughput* dari ketiga algoritma dapat digunakan sebagai referensi dan pengembangan aplikasi pengaman berkas digital lainnya, serta pemilihan bahasa pemrograman yang sesuai untuk mengoptimalkan kinerja dari ketiga algoritma tersebut.
2. Untuk mengatasi masalah *memory leak* dan *memory fragmentation*, sebaiknya pada saat membuat program algoritma kriptografi dengan C# yang menggunakan platform .Net 4.5.50709, program tersebut memakai *garbage collector* yang ada pada System.GC.

UMMN