

Bab 5 PENUTUP

5.1 Kesimpulan

Berdasarkan hasil dari pengujian penerapan Algoritma AES dan RSA pada data yang akan di *upload* ke *cloud storage* maka dapat ditarik kesimpulan sebagai berikut:

1. Pengembangan sistem pengamanan file yang akan disimpan ke *cloud storage* menggunakan algoritma AES dan RSA dilakukan dengan dua tahapan penting, Tahapan pertama yang harus dilakukan adalah membuat proses enkripsi dan dekripsi terlebih dahulu dengan menggunakan AES untuk mengenkripsi dan mendekripsi isi dari file dan menggunakan RSA untuk mengenkripsi kunci dari AES. Tahapan selanjutnya adalah menghubungkan proses enkripsi dekripsi tersebut dengan *cloud storage* yang digunakan. Dalam penelitian ini yang digunakan adalah Google Drive dan Dropbox.
2. Kinerja sistem yang menggunakan Algoritma AES dan Algoritma RSA serta dua *Cloud Storage* (Google Drive dan Dropbox) dapat berjalan dengan baik, hanya dibagian *download* dan dekripsi file bisa lebih dikembangkan lagi agar lebih efisien.
3. Pada proses enkripsi dan dekripsi file semakin besar ukuran file maka akan semakin lama juga waktu enkripsi dan dekripsi. Dan proses enkripsi hanya menambah beberapa *bytes* pada file. Serta koneksi internet menjadi faktor terbesar yang mempengaruhi waktu *upload*.

Isi dan ukuran file tidak berubah antara file asli dengan file yang sudah dilakukan enkripsi dan dekripsi. Keamanan file yang disimpan di *cloud storage* juga aman karena file tersebut tidak bisa dibaca jika tidak dienkripsi terlebih dahulu.

5.2 Saran

Berdasarkan hasil dari sistem dan dari kesimpulan diatas dapat saran yang dapat diberikan kepada peneliti selanjutnya adalah sebagai berikut:

1. Perlunya memperbaiki proses *download* file dan dekripsi agar sistem bisa bekerja dengan lebih efisien
2. Perlunya pengembangan tampilan antarmuka karena tampilan antarmuka pada sistem ini sangatlah tidak menarik.