BAB V

KESIMPULAN DAN SARAN

5.1. Kesimpulan

Dari penelitian yang dilakukan, dapat disimpulkan bahwa aplikasi yang mengimplementasikan algoritma kriptografi ElGamal dan kompresi LZW berhasil dibangun. Dengan menggunakan aplikasi ini, pengguna dapat mengamankan dokumen digitalnya dengan mengenkripsi.

Apabila dilihat dari hasil pengujian aplikasi terlihat bahwa performa algoritma kriptografi ElGamal tidak terlalu cepat, karena untuk memroses dokumen berukuran 13 MB membutuhkan waktu lebih dari dari 5 menit baik pada saat enkripsi maupun dekripsi. Algoritma kompresi LZW terlihat kurang begitu efektif digunakan dengan algoritma kriptografi ElGamal. Hal ini terbukti dengan ukuran data hasil kompresi yang lebih besar dari data sebelum dikompresi. Tetapi jika dilihat dari segi keamanan, maka algoritma ini dapat disebut berhasil karena berkas yang dienkripsi tidak berhasil dibuka dengan aplikasi yang digunakan untuk membuka berkas sebelum dienkripsi (beberapa menyatakan terdapat kerusakan pada berkas). Hal ini menandakan bahwa data telah sepenuhnya terenkripsi.

5.2. Saran

Beberapa saran yang diajukan terhadap penelitian ini adalah sebagai berikut.

1. Pengimplementasian algoritma kompresi. Seperti yang telah dijelaskan bahwa salah satu kelemahan pada algoritma kriptografi ElGamal ini adalah ukuran

file hasil enkripsi yang terlalu besar. Algoritma LZW dirasa kurang efektif dalam mereduksi beban data yang dihasilkan oleh algoritma ElGamal. Oleh karena itu, untuk lebih menyempurnakan penggunaan algoritma ini dapat dicoba untuk mengimplementasikan algoritma kompresi lain yang dapat mereduksi beban data yang lebih baik.

2. Pengimplementasian bahasa pemrograman. Bahasa pemrograman C# masih cukup populer digunakan dalam pembangunan aplikasi berbasis desktop. Pada penelitian ini aplikasi dirasakan kurang stabil, karena jika memroses *file* yang berukuran lebih dari 5 MB maka terkadang aplikasi akan berhenti merespon. Oleh karena itu , jika dimungkinkan, lebih baik dapat dicoba untuk membangun aplikasi yang serupa (atau mengimplementasikan algoritma kriptografi ElGamal) dengan menggunakan bahasa pemrograman yang lain. Karena mungkin dengan bahasa pemrograman yang lain akan didapatkan aplikasi yang lebih stabil.
3. Pembangunan aplikasi berbasis mobile. Seperti yang kita tahu bahwa perkembangan didunia teknologi mengarah kepada aplikasi berbasis mobile. Akan sangat bagus jika algoritma ElGamal ini dapat diaplikasikan pada mobil, mengingat tingkat kemanannya yang cukup tinggi.
4. Pengembangan dapat dilakukan dengan mencoba untuk melakukan proses enkripsi dan dekripsi pada dokumen-dokumen digital lain, seperti gambar, *audio*, dan *video*. Oleh karena itu, pembatasan masalah dapat ditambahkan dengan file-file ber-ekstensi (.jpg), (.jpeg), (.bmp), (.png), (.wav), (.avi), (.flv), dan lain-lain.

5. Skenario yang lain. Pada laporan skripsi ini, skenario yang dilakukan adalah ekripsi-kompresi dan dekompresi-dekripsi. Pengembangan aplikasi dapat dilakukan dengan mencoba skenario yang berbeda, seperti kompresi-enkripsi dan dekripsi-dekompresi.