BAB V

PENUTUP

5.1 Kesimpulan

Berdasarkan hasil analisis dan implementasi yang telah dilakukan pada bab-bab sebelumnya, serta untuk mengakhiri penelitian pada laporan skripsi yang berjudul **"Implementasi Algoritma Kriptografi Hybrid (DES, AES, dan ElGamal) Pada Aplikasi Desktop Berbasis Phyton"**, maka dapat diambil kesimpulan sebagai berikut:

1. Aplikasi ini sudah dirancang sedemikian rupa agar dapat mengenkripsi dan mendekripsi pesan tanpa harus melalui langkah-langkah panjang. Jadi, proses enkripsi dan dekripsi ini sudah secara otomatis dijalankan oleh komputer tanpa harus menampilkan kepada user bagaimana proses ini berjalan.
2. Pada aplikasi ini, *ciphertext* yang dihasilkan merupakan hasil yang diberi *Initial Vector* (IV). Dimana IV merupakan random input supaya hasil enkripsi (*ciphertext*) terlihat berbeda walaupun *plaintext* dan *key* sama.
3. Pada aplikasi ini juga, *ciphertext* yang dihasilkan merupakan *serialize* objek python ke string mengunakan pickle.
4. Algoritma DES membatasi panjang kunci/*password* untuk proses enkripsi dan dekripsi. Oleh karena itu, untuk dapat mengenkripsi dan mendekripsi hanya dapat menggunkan 8 karakter saja.
5. Algoritma *Hybrid* (DES + ElGamal maupun AES + ElGamal) dalam proses enkripsi dan dekripsi memiliki kinerja atau proses yang lama karena menggunakan *asymmetric encryption* dimana proses komputerisasi yang lebih banyak. Untuk mempercepat proses dapat dikurangi nilai *key*-nya,

tetapi kalau dikurangi *key*-nya maksimum karakter yang dapat dienkripsi juga akan semakin kecil.

5.2 Saran

Dalam penulisan skripsi ini tentunya masih terdapat banyak kekurangan, namun tidak menutup kemungkinan untuk dapat disempurnakan untuk pengembangan selanjutnya serta dapat meningkatkan fungsional dan manfaat aplikasi ini. Beberapa hal yang mungkin dapat dilakukan untuk pengembangan aplikasi PyCryptoTools ini yaitu:

1. Menambahkan tutorial dalam aplikasi agar lebih dapat memperjelas proses yang akan digunakan.
2. Memperbaiki *Graphical User Interface* (GUI) agar lebih menarik dan lebih *user friendly*.
3. Menambahkan proses penyimpanan proses-proses enkripsi dan dekripsi yang sudah dilakukan agar mudah dalam pengiriman pesan.