

BAB V

PENUTUP

5.1 Kesimpulan

Dari pengujian dan hasil evaluasi yang dilakukan pada aplikasi dapat diambil kesimpulan sebagai berikut :

1. Aplikasi *chatting* (*java applet*) yang berjalan pada website tidak dapat melakukan enkripsi pada file. Hal ini disebabkan policy standart keamanan aplikasi *java applet*. *Applet* secara default tidak diperkenankan untuk membaca dan menulis suatu *file*.
2. Dari hasil pengujian diketahui bahwasannya data yang dikirimkan melewati jaringan telah terenkripsi, sehingga orang *sniffer* (penyadap) tidak dapat membaca data pesan tanpa mengetahui algoritma dan kunci yang digunakan.
3. Program aplikasi yang dibuat penulis mampu bekerja seperti yang diharapkan dalam hal ini mampu melakukan proses enkripsi terhadap pesan user. Adapun pesan yang berupa *plain text* dienkripsi dengan menerapkan algoritma RSA atau IDEA. Untuk data berupa *file* dienkripsi menggunakan algoritma IDEA.
4. Enkripsi data berupa *file* ditentukan menggunakan algoritma IDEA yang merupakan jenis *symmetric encryption*, pemilihan algoritma enkripsi dilakukan dengan memperhatikan dengan waktu proses enkripsi *file*.
5. Waktu proses algoritma enkripsi RSA untuk enkripsi data *plaintext* maupun *file* lebih lambat jika dibandingkan algoritma enkripsi IDEA.
6. Data hasil enkripsi dengan algoritma enkripsi RSA lebih panjang/banyak dan tidak efisien jika dibandingkan algoritma enkripsi IDEA.

5.2 Saran – Saran

Saran – saran yang dapat diberikan oleh penulis untuk penelitian ataupun pengembangan Tugas Akhir ini :

1. Sistem yang dibuat dapat dikembangkan dengan menambahkan algoritma enkripsi yang dapat diterapkan pada aplikasi *chatting*.
2. Untuk mendapatkan performance yang terbaik sebaiknya menggunakan algoritma enkripsi dengan tipe *symmetric encryption*.
3. Untuk memaksimalkan penambahan fitur pada aplikasi *chatting* dengan memperhatikan sisi keamanan, sebaiknya aplikasi *chatting* hanya menggunakan aplikasi desktop.

STIKOMMP SURABAYA