BAB V

PENUTUP

5.1. Kesimpulan

Setelah menyelesaikan perangkat lunak simulasi *man in the middle attack* pada algoritma kriptografi RSA dan pencegahannya dengan *interlock protocol*, penulis menarik kesimpulan, bahwa:

1. Pembangkitan kunci algoritma RSA supaya mendapatkan bilangan prima besar untuk meningkatkan kekuatan kunci maka dilakukan dengan pembangkitan bilangan acak secara random oleh perangkat lunak.
2. Dengan menggunakan *interlock protocol*, walaupun kunci publik pihak penerima dan pengirim didapatkan dan diganti oleh penyadap, tetapi penyadap tidak dapat menjalankan prosedur *man-in-the-middle-attack* untuk melihat dan mengubah pesan. Hal ini dikarenakan pesan terenkripsi terbagi menjadi dua bagian pada variasi pertama dan terdapat fungsi *hash* untuk memverifikasi keaslian pesan pada variasi kedua.
3. Perangkat lunak mensimulasikan proses kerja *man-in-the-middle-attack* sebagai salah satu bentuk penyerangan terhadap metode kriptografi publik dan proses kerja *interlock protocol* untuk mengatasinya, sehingga perangkat lunak dapat digunakan untuk mendukung proses belajar mengajar, terutama dalam mata kuliah Kriptografi.

4. Pendeteksian keberadaan penyadap tidak diketahui jika tidak terjadi modifikasi dalam isi pesan yang dikirim.
5. Noise yang timbul disebabkan faktor teknis pada jaringan atau non-teknis selama pengiriman data, tidak dikategorikan sebagai adanya penyadapan walaupun terdapat jeda antara pengiriman pesan bagian 1 dan 2 saat dilakukan simulasi interlock protocol

5.2 Saran

Sebagai saran pengembangan dari selesainya perancangan simulasi *man in the middle attack* pada algoritma kriptografi RSA dan pencegahannya dengan *interlock protocol*, penulis berharap bahwa:

1. Perangkat lunak ini dapat dikembangkan dengan menambahkan algoritma kunci publik lainnya, seperti: metode Rabin atau ElGamal.
2. Perangkat lunak dapat dikembangkan dengan menambahkan fitur condition, dimana mensimulasikan keadaan-keadaan yang mungkin terjadi pada media jaringan, seperti cuaca, overload server dan lainnya.
3. Penambahan jumlah input-an pesan lebih dari 50 karakter agar dapat memuat panjang kalimat.