BAB V

KESIMPULAN DAN SARAN

5.1 Kesimpulan

Setelah menyelesaikan perangkat lunak simulasi pencegahan *man-in-the-middle attack* dengan *interlock protocol*, penulis menarik kesimpulan sebagai berikut:

1. 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.
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.

5.2 Saran

Penulis ingin memberikan beberapa saran yang mungkin dapat membantu dalam pengembangan perangkat lunak ini yaitu :

1. Perangkat lunak ini dapat dikembangkan dengan menambahkan algoritma kunci publik lainnya, seperti: metode Rabin, ElGamal dan LUC.
2. Perangkat lunak dapat dikembangkan dengan menambahkan fitur *multimedia*, yaitu dengan menambahkan animasi yang lebih baik dan suara yang mendukung proses simulasi.

DAFTAR PUSTAKA

Bhansali,Bhavin Bharat, 2001, *Man-In-The-Middle-Attack*, SANS Institute 2000-2002, http://www.giac.org/certified_professionals/practicals/gsec/0455.php, Tanggal Akses 28 Februari 2008 Pukul 14:40 WIB

Fithria, Naila, *Jenis-jenis Serangan Terhadap kriptografi*, Tugas Akhir Matematika Diskrit, Jurusan Teknik Informatika ITB, Bandung,http://mail.informatika.org/~rinaldi/Matdis/2007-2008/Makalah/MakalahIF2153-0708-050.pdf, Tanggal Akses 22 Februari 2008 Pukul 16:49 WIB

Kamal, Tahiri Jouti, 2004, *Primality Testing*, B.Kaufmann

Kurniawan, Jusuf, 2004, *Keamanan Internet dan Jaringan Komunikasi*, Penerbit Informatika Bandung

Laba Kuma, Gervasius, 2008, *Implementasi Stegeanografi untuk menyisipkan Data Teks, Gambar dan Audio pada File Gambar Bertipe Bitmap*, STMIK AKAKOM Yogyakarta

Malik, Jaja Jamaludin, 2007, *Kumpulan Tip dan Trik Pemrograman Visual Basic*, Penerbit Andi Yogyakarta

Munir, Rinaldi, 2006, *Kriptografi*, Penerbit Informatika Bandung, Bandung

Putra, Rahmat, 2006, *Visual Basic All Version (Innovative Source Code),* Dian Rakyat, Jakarta

Satriyo Hasan Nurdin & Faisol Amir, *Network security*, PENS-ITS, http://kebo.vlsm.org/mediawiki1.9/index.php/Network_security, Tanggal akses 22 Maret 2008, pukul 01:44 WIB

Scheneier, Bruce, 1996, *Applied Cryptography*, Second Edition; John Wiley and Sons, Inc., Canada

_____,_____, *Modular exponentiation*, http://en.wikipedia.org/