ABSTRACTION

RSA cryptograph method is relatively safe to use and applied in many fields of work to save data communication. But it probably occurs a tapping process towards data. One of the tapping forms is *man in the middle attack* problem.

Man-In-The-Middle-Attack is a term used for tapping process towards media of communication. The condition draws that the tapper is between both communicans so the data must be stored by the tapper and he knows all of the information.

Nowadays, the problem of *Man-In-The-Middle-Attack* can be encountered by the *interlock protocol* method. The main algoritma of this protocol is by sending two parts of encrypted messages. It causes the tapper can not describe the first message by using its private key. It can only create a new message and send it to the message receiver.

This stimulate soft ware is made to facilitate the users in understanding the process of *Man-In-The-Middle-Attack* and *Interlock Protocol* easily as an effort to encounter this kind of tapping process. Designed methodology of the thesis uses linier sequential approach and its implementation uses language of Visual Basic 6 program.

Key words are RSA cryptograph, *man-in-the-middle-attack, Interlock Protocol.*

ABSTRAKSI

Metode kriptografi kunci public RSA relatif aman dan banyak diaplikasikan dalam upaya pengamanan komunikasi data, namun ternyata masih terjadi penyadapan terhadap data yang dikirimkan, salah satu bentuk penyadapan yang ditemukan adalah problema *man-in-the-middle-attack.*

Man-In-The-Middle-Attack adalah istilah untuk jenis penyadapan terhadap media komunikasi, kondisinya pihak penyadap berada diantara kedua pihak yang berkomunikasi dan data yang dikirimkan selalu melalui pihak yang menyadap, sehingga pihak penyadap dapat mengetahui semua informasi yang dikirimkan.

Tapi saat ini problema *man-in-the-middle-attack* dapat ditangani dengan metode *interlock protocol.* Algoritma inti protokol ini ialah mengirimkan 2 bagian pesan terenkripsi, ini menyebabkan pihak yang menyadap tidak dapat mendekripsi pesan pertama dengan menggunakan kunci privatnya, dia hanya dapat membuat sebuah pesan baru dan mengirimkannya kepada pihak yang akan menerima pesan tersebut.

Perangkat lunak simulasi ini dibuat untuk membantu pengguna agar menjadi lebih mudah memahami proses terjadinya problema *man-in-the-middle-attack* dan proses *Interlock Protocol.* Metodologi rekayasa pada tugas akhir ini menggunakan pendekatan sekuensial linear sedangkan implementasinya menggunakan bahasa pemrograman Visual Basic 6.

Kata kunci : kriptografi RSA, *man-in-the-middle-attack, Interlock Protocol.*