ABSTRAK

Dalam dunia sekarang ini, kemajuan teknologi di bidang komputer dan telekomunikasi berkembang sangat pesat. Lalu lintas pengiriman data dan informasi yang semakin global, serta konsep *open system* dari suatu jaringan memudahkan seseorang untuk masuk ke dalam jaringan tersebut. Hal tersebut dapat membuat proses pengiriman data menjadi tidak aman dan dapat saja dimanfaatkan oleh pihak lain yang tidak bertanggung jawab, yang mengambil informasi atau data yang dikirimkan tersebut di tengah perjalanan. Maka dibutuhkan suatu sistem keamanan yang dapat menjaga kerahasiaan suatu data, sehingga data tersebut dapat dikirimkan dengan aman. Salah satu solusi untuk menjaga keamanan dan kerahasiaan pada proses pengiriman data dengan menggunakan teknik kriptografi.

Kriptografi telah menjadi suatu bagian yang tidak dapat dipisahkan dari sistem keamanan jaringan antar komputer yang juga merupakan salah satu solusi agar informasi atau pesan yang dikirim dalam suatu jaringan tidak dapat dimanfaatkan oleh pihak lain. Kriptografi akan mengubah informasi yang dikirim menjadi suatu pesan yang tidak memiliki makna, dan tidak dapat dimengerti oleh pihak lain selain penerima.

Dalam tugas akhir ini penulis merealisasikan suatu perangkat lunak enkripsi dan dekripsi file teks dengan menggunakan algoritma kriptografi yaitu FEAL. Di samping itu untuk meningkatkan keamanan pada perangkat lunak disertakan juga proses validasi dan proses *digital signature*, sehingga perangkat lunak dapat mendeteksi adanya perubahan data atau informasi yang dikirimkan serta menjamin keaslian pengirim informasi. Perangkat lunak ini dibuat dengan menggunakan bahasa pemrograman Microsoft Visual Basic 6.0.

ABSTRACT

In the world today, the development of technology in the sector of computer and telecommunication has grown fast. The traffic of sending data and global information, also open system concept from a certain network make someone easier to go into that network. It can make a data shipping process does not save and can be exploited by other side who do not have any responsibility, who take an information or data which will be sent on the way. So, it is needed a security system able to take care of data secret, so that the data can be sent safely. One of the solution to take care of secret and security at process delivery of data by using a cryptography technique.

Cryptography has become certain parts which cannot be separated from a network security system between computer and also a part of solution in order that information or message which is sent in a network cannot be exploited by other people. Cryptography will change a sending information become an unmeaning message, and cannot be understood by other people but receiver.

In this final thesis, encryption and decryption file using FEAL algorithm has realized.. Beside that, not only to improve the security level, in the software also included validation and digital signature process, so that software is able to detect the text changes and able to guarantee the originality of sender of massage. The software of FEAL is made by using Microsoft Visual Basic 6.0 language program.

DAFTAR ISI

DAFTAR GAMBAR

DAFTAR TABEL