ABSTRAK

Masalah keamanan dan kerahasiaan data merupakan salah satu aspek yang sangat penting dalam era informasi sekarang ini. Salah satu solusi untuk mengatasinya adalah dengan melakukan enkripsi (penyandian) terhadap data yang akan dikirimkan dengan waktu penyandian yang tidak lama.

Dalam menyandikan suatu data dan menerjemahkannya kembali digunakan suatu data yang disebut kunci. Algoritma enkripsi yang didasarkan pada kunci secara garis besar dibedakan menjadi dua macam, yaitu algoritma simetrik dan algoritma kunci publik (algoritma asimetrik). Algoritma yang digunakan pada tugas akhir ini adalah algoritma simetrik yaitu penyandian dengan menggunakan kunci yang sama untuk enkripsi dan dekripsi data yang disebut dengan *secret key*.

Tugas Akhir ini akan merealisasikan suatu perangkat lunak pengaman data dengan algoritma simetrik menggunakan metode enkripsi RC2. Perangkat lunak ini dibuat dalam bahasa pemrograman *Borland Delphi*. Perangkat lunak yang direalisasikan mempunyai 7 Bagian utama yaitu : Inisialisasi RC2 dan *Mixing* S-Box, Enkripsi *Plaintext,* Pembangkit Kunci Tanda Tangan Digital, Validasi dan Tanda Tangan Digital, Dekripsi *Ciphertext, Open Decipehered Text, dan* membuat *plaintext* dan *ciphertext* data.

ABSTRACT

Nowadays in the age of information, the problems of data security and secrecy are one of the most important aspects on computer communication and networks. One of the solutions to handling these problems is data encoding (encryption) with a short time in encoding and decoding.

Some keys are used when encoding data and decoding it back to its original data. There are two general types of the algorithm, symmetric algorithm and public key algorithm. Algorithm used on this book is symmetric algorithm. Symmetric algorithm is designed so that the key use for encryption is the same as the key used for decryption which is called secret key.

Data protection software with symmetric algorithm using RC2 Encryption that realized in this book is made with Borland Delphi programming language. This software consists of 7 main parts which are: Initializes RC2 and Mixing S-Box, Plaintext encryption, Digital Signature key generator, Validation and Digital Signature, Cipher text decryption, Open Deciphered Text, and create *plaintext* and cipher text.

DAFTAR ISI

DAFTAR GAMBAR

DAFTAR TABEL