INTISARI

Kriptogafi adalah sebuah seni dan bidang keilmuan dalam penyandian informasi atau pesan dengan tujuan menjaga keamanannya. Salah satu jenis kriptografi adalah kriptografi Blowfish. Kriptografi Blowfish merupakan metode enkripsi dekripsi 64-bit yang mirip dengan DES (*Des Like Cipher*) dan diciptakan oleh Bruce. Blowfish dikembangkan untuk memenuhi kriteria desain yang cepat, kompak, sederhana dan aman.

Program dibuat dengan algoritma Blowfish terdiri dari tiga proses, yaitu subkunci, proses enkripsi (penyandian dari *plaintext* ke *ciphertext*), proses dekripsi (penyandian dari *ciphertext* ke *plaintext*). Proses subkunci, pesan asli di-XOR-kan dengan PBox yang telah diinisialisasi kemudian dilakukan modifikasi dengan masukan *string* 0. Pada proses enkripsi pesan asli dikenakan jaringan feistel dan diputar sebanyak 15 kali putaran, sedangkan untuk proses dekripsi kebalikan dari proses enkripsi yang juga dikenakan jaringan feistel dan diputar sebanyak 16 kali putaran.

Dari hasil perancangan dan pengamatan menunjukkan program penyandi enkripsi dan dekripsi dengan algoritma Blowfish berhasil menyandikan data 64 bit dan program algoritma Blowfish mampu menampilkan pesan asli dan pesan yang telah disandikan.

Kata kunci : enkripsi, dekripsi, *subkey*, *plaintext*, *ciphertext*, jaringan feistel

ABSTRACT

Cryptography is an art an subject knowledge in information coding or messages with purpose to keep it's security. Kind of cryptography is Blowfish cryptography. Blowfish cryptography is 64-bit description encryption metod whichis like with DES (Des Like Chiper) and created by Bruce Sheiner. Blowfish develop for fulfil design criteria with is fast, compact, simple and secure.

This program made by Blowfish algorithm consist of three is subkey, procces is encryption (coding from *plaintext* to *chipertext*), procces is decryption (coding from *chipertext* to *plaintext*). At the *subkey* procces, original messages is XOR-ed by PBox which was inisialed then it is modified by entering zero 0 string. There is feistel network at original message in encryption procces and 15 times turned, description procces is the opponent of encryptionwith is also use feistel network and turned 16 times.

From design result and observation are show that encryption decryption coding program with Blowfish algorithm are success to code 64 data and Blowfish algorithm program is able to show original messages and coded messages.
Keyword: encryption, decryption, subkey, *plaintext*, *chipertext*, feistel network