ABSTRAK

Kriptografi merupakan cara untuk menyandikan sebuah pesan. Kriptografi digunakan untuk menjaga pesan secara rahasia, menjaga integritas data, serta untuk menjamin otentikasi seseorang atau informasi. Proses kriptografi terdiri atas proses enkripsi yaitu suatu metode untuk mengubah pesan asli (*plaintext*) menjadi suatu pesan acak (*ciphertext*), dan proses dekripsi yaitu metode yang digunakan untuk mengubah *ciphertext* menjadi *plaintext*.

Terdapat tiga jenis algoritma didalam kriptografi yaitu algoritma kunci pribadi, algoritma kunci *public* dan algoritma *hash*. Algoritma kunci pribadi menggunakan sebuah kunci yang sama untuk proses enkripsi dan dekripsi. Algoritma kunci *public* menggunakan dua buah kunci yang berbeda yaitu kunci pribadi dan kunci *public*. Algoritma *hash* menggunakan fungsi hash untuk mendapatkan ciphertext sehingga tidak dibutuhkan kunci.

Algoritma Blowfish bekerja secara *block cipher*, dimana data yang dimasukkan akan dibagi kedalam blok-blok yang berukuran 64 bit. Proses enkripsi dan dekripsi dilakukan tiap blok, dimana blok yang berukuran 64 bit tersebut akan dibagi menjadi XL dan XR yang masing-masing berukuran 32 bit. Selanjutnya XL dan XR tersebut akan dipermutasi sebanyak 16 putaran.

Algoritma Blowfish sangat baik dalam menjaga keamanan data karena menggunakan kunci yang panjangnya dapat mencapai 448bit. Algoritma Blowfish ini juga mudah diimplementasikan karena algoritmanya sederhana dan operasi yang digunakan hanya operasi AND dan XOR. Selain itu Blowfish juga cepat dalam melakukan proses enkripsi dan dekripsi.

ABSTRACT

Cryptography is a method of message writing secretly. Cryptography is used to keeping a message secretly, keeping the data integrity, and proving someone's or message's identity. The cryptography process consist of encryption that is a method to alter the original message (plaintext), into a random message (ciphertext), and the decryption process is a method which used to alter ciphertext into plaintext.

There are three kinds of algorithm in cryptography that is secret-key algorithm, public-key algorithm, and hash algorithm. Secret-key algorithm is an algorithm that uses a same key for encryption and decryption process. Public-key algorithm is an algorithm that uses two different keys, private key and public key. Hash algorithm.

Blowfish algorithm is an algorithm that works in block cipher, in which the data input will be divided into blocks of 64 bit. The encryption and decryption process of this algorithm is performed for each block, in which the 64bit-block will be divided into XL and XR, each of which is 32 bit. Next, those XL and XR will permutated as many as 16 rotation.

Blowfish algorithm is very reliable to keep data security because the input using a key which has length to 448 bit. Blowfish algorithm is also easy to implementation because Blowfish algorithm is simple and the operation are use AND operation and XOR operation. Beside that, Blowfish algorithm can do the process of encryption and decryption quickly.