Ardi Juliardi (13360010), Rancang Bangun Aplikasi Enkripsi DAN Dekripsi Pada Database SQL Permikomas Menggunakan Algoritma Blowfish, Jakarta: Program Studi Teknik Informatika, FSTI, ISTN, Agustus 2018.

Abstrak

Untuk menjaga keamanan data ataupun informasi yang tersimpan dalam *database* SQL adalah dengan menggunakan enkripsi. Ada banyak algoritma enkripsi yang ada dan salah satunya adalah algoritma *Blowfish*. Algoritma *Blowfish* merupakan algoritma modern kunci simetris berbentuk *chiperblock*. Enkripsi dilakukan dengan menggunakan kunci tertentu, sehingga menghasilkan *chipertext* yang tidak bisa dibaca. *Chipertext* tersebut dapat dikembalikan seperti semula jika didekripsi menggunakan kunci yang sama.

Algoritma *Blowfish* memiliki 16 putaran dan masukan berupa data 448 bit. Bagi data 448 bit tersebut menjadi 2 bagian XL dan XR yang masing-masing 224 bit, selanjutnya lakukan operasi XL = XL xor Pi dan XR = F(XL) xor XR, kemudian tukar XL dan XR, lakukan proses sebanyak 16 kali. Pada proses ke-17 lakukan operasi untuk XR = XR xor P17 dan XL = XL xor P18, kemudia satukan kembali XL dan XR sehingga menjadi 448 bit kembali sehingga menghasilkan *chipertext*.

Dari penggunaan algoritma Blowfish ini membuat data dari *database* SQL yang meliputi *database*, *table*, *field*, dan *record* tidak dapat terbaca karena telah terenkripsi, sehingga hanya *user* tertentu yang dapat membaca isi dari *database* dengan cara mendekripsinya.

Kata Kunci: Algoritma *Blowfish*, enkripsi, dekripsi, kunci simetris.

Ardi Julinrdi (13360010), Rancang Bangun Aplikasi Enkripsi DAN Dekripsi Pada Database SQL Permikomas Menggunakan Algoritma Blowfish, Jakarta: Informatics Engineering Study Program, FSTI, ISTN, August 2018

Abstract

To maintain the security of data or information stored in the SQL database is to use encryption. There are many existing encryption algorithms and one of them is the Blowfish algorithm. Blowfish algorithm is a modern algorithm of symmetrical keys in the form of chipertext. Encryption is done by using a certain key, resulting in an unreadable chipertext. The chipertext can be returned as if it were decrypted using the same key.

Blowfish algorithm has 16 rounds and input is 448 bit data. Divide the 448 bit data into 2 parts XL and XR each 224 bit, then do XL = XL Xor Pl and XR = F (XL) xor XR, then exchange XL and XR, do the process 16 times. In the 17th process do the operation for XR = XR xor P17 and XL = XL xor P18, then reconnect XL and XR so that it becomes 448 bits back to produce a chipertext.

The use of Blowfish algorithm makes data from SQL databases that include databases, tables, fields, and records can not be read because they are encrypted, so that only certain users can read the contents of the database by decrypting them.

Keywords: Blowfish algorithm, encryption, decryption, *symmetric keys.*