INTISARI

MD5 merupakan salah satu contoh algoritma hash yang hampir sama dengan proses enkripsi tetapi tidak dapat digunakan untuk proses dekripsi. Algoritma MD5 ini dikembangkan oleh Profesor Ronald Rivest pada tahun 1991. Algoritma MD5 telah berkembang pesat dalam berbagai aplikasi karena tingkat keamanan, kecepatan dan sederhana dalam design.

Sistem ini dibangun untuk dua pihak, yaitu pihak pengguna (*client*) dan pihak administrator (*server*). Untuk menghubungkan ke-dua pihak tersebut digunakan protokol Challenge-Response. Cara kerja protokol Challenge-Response yaitu server menyediakan dan memberi challenge, sedangkan client mengolah challenge dan memberi response. Protokol Challenge-Response digunakan dalam beberapa aplikasi yang menghindarkan adanya transfer password secara langsung.

Tujuan dari Tugas Akhir ini adalah mengimplementasikan algoritma MD5 dengan protokol Challenge-Response untuk melakukan hash masukan berupa password yang telah di hash, yang akan disambung dengan Challenge. Hasil implementasi berupa kode hash yang berbeda walaupun dengan Challenge yang sama dan algoritma yang sama.

ABSTRACT

MD5 is one of any other hash algorithms looks like encryption, but can't do decryption. It was created by Professor Ronald Rivest in 1991. MD5 have been developed in many applications because of the safety, quickly in processing and simplicity in design.

The system was built for two sides, namely client side and server side. Challenge-Response Protocol is used to connect them. In Challenge-Response Protocol, server will provide and give challenge, in the other hand client will generate challenge and sent response. Challenge-Response Protocol is used in any applications to avoid the transfer password directly.

The purpose of this final assignment is to see the implementation of MD5 algorithm using Challenge-Response Protocol for hashing input like a hashed password concated by challenge. The output of this implementation like hash code and never equal although using the same challenge and the same algorithm.