ABSTRACT

The importance value of information can cause frequently information which can only be accessed by certain people, fall to other party so that they can cause loss to information owner. To ensure that user is true one who is permitted, needed an authentication system, such as password authentication system. The technique is cryptography. This Final Project discusses about cryptography related password secret that is key derivation function.

Crypt MD5 is one of key derivation functions which processing password and salt string input using MD5 algotithm looping to produce output. Crypt MD5 algorithm uses 64 bit salt and 1000 main iteration. Crypt MD5 compression function is equal to MD5 compression function. Main output is 132 bit and it uses transformation base64 for output representation.

With usage of Crypt MD5 algorithm for password authentication password, will improve security by complicating revealed password effort.

Key words : password, hash function, key derivation function, encrypt, *Crypt MD5.*