ABSTRAK

Sangat pentingnya nilai sebuah informasi menyebabkan sering kali informasi yang hanya boleh diakses oleh orang-orang tertentu, jatuh ke pihak lain sehingga dapat menimbulkan kerugian bagi pemilik informasi. Untuk memastikan bahwa pengguna adalah benar orang yang berhak diperlukan sistem autentikasi, seperti sistem autentikasi password. Teknik yang digunakan adalah kriptografi. Tugas Akhir ini membahas mengenai kriptografi yang berkaitan dengan kerahasiaan password yaitu fungsi derivasi kunci.

Crypt MD5 adalah salah satu fungsi derivasi kunci yang memproses input string password dan salt menggunakan perulangan algoritma MD5 untuk menghasilkan output. Algoritma Crypt MD5 ini menggunakan salt sepanjang 64 bit dan 1000 kali iterasi utama. Fungsi kompresi Crypt MD5 sama dengan fungsi kompresi MD5. Output utama yang dihasilkan sepanjang 132 bit dan menggunakan transformasi base64 untuk representasinya.

Dengan penggunaan algoritma Crypt MD5 untuk sistem autentikasi password ini, akan meningkatkan keamanan dengan menyulitkan usaha pembobolan password.

Kata Kunci : password, fungsi hash, fungsi derivasi kunci, enkripsi, *Crypt MD5*.