

Aplikasi Kriptografi sederhana menggunakan fungsi Hashing (MD5) pada modul PHP

Deskripsi Lengkap: <https://lib.ui.ac.id/detail?id=20435891&lokasi=lokal>

Abstrak

Jaringan komputer memungkinkan terjadinya kegiatan pertukaran data dari satu komputer ke komputer lain. Ada beberapa persoalan penting dalam proses pengiriman dan penerimaan data dalam jaringan komputer, yaitu keamanan data (kerahasiaan, otentikasi, integritas, non-repudiasi). Persoalan tersebut dapat diatasi dengan kriptografi menggunakan MD5 (message Digest 5). MD5 merupakan pengembangan dari algoritma fungsi hash yang memberikan jaminan bahwa data yang dikirimkan akan sama dengan data yang diterima. Bahasa pemrograman yang berbasis komputer yang menyediakan fungsi hash salah satunya adalah PHP. PHP memiliki prosedur standar untuk mengamankan data-data pada jaringan komputer berupa library khusus untuk mengenkripsi data. Dalam PHP dikenal dua library enkripsi, yaitu MCRYPT dan MHASH. Pada penelitian ini akan dibuat sebuah aplikasi untuk mengenkripsi data berupa string menggunakan fungsi hash MD5 dengan memanfaatkan library PHP, yaitu MHASH.