Kelompok 7:

1. Ilham Jody Bimantara (07)
2. M. Khusuma Dwi N (12)
3. Monalisa Desideria M (13)
4. Yogie Tri Priyo S (22)

# Revisi Presentasi Pemrograman Basis Data

# Hash dan Enkripsi

## Pengertian Hash

**Hash** adalah sebuah algoritma yang mengubah sebuah data informasi berupa huruf, angka atau karakter lainnya menjadi karakter terenkripsi dengan ukuran yang tetap, data yang sudah di enkripsi melalui fungsi hash tidak dapat dikembalikan atau didekripsi. Oleh karna itu, Hash bisa disebut dengan One Way Function atau bisa juga dikatakan enkripsi yang satu arah. Fungsi hash itu sendiri biasa nya dimanfaatkan untuk *Password Hashing* (Menyembunyikan Password Asli) atau *Digital Signature* (Tanda tangan digital). Algoritma hash yang umum digunakan yaitu MD5 dan SHA1.

MD5 adalah fungsi hash yang digunakan secara luas dengan hash value 128-bit. Pada standart Internet (RFC 1321), MD5 telah dimanfaatkan secara bermacam-macam pada aplikasi keamanan. “MD” adalah singkatan dari “Message Digest.”

SHA-1 (Secure Hash Algorithm 1) adalah fungsi hash kriptografi yang mengambil input dan menghasilkan nilai hash 160-bit (20-byte) yang dikenal sebagai intisari pesan — biasanya ditampilkan sebagai angka heksadesimal, panjang 40 digit. Ini dirancang oleh Badan Keamanan Nasional Amerika Serikat (NSA), dan merupakan Standar Pemrosesan Informasi Federal A.S.

## Pengertian Enkripsi

**Enkripsi** adalah proses mengamankan suatu informasi dengan membuat informasi tersebut tidak dapat dibaca tanpa bantuan pengetahuan khusus. Proses kebalikannya disebut **Dekripsi**, yaitu proses untuk membaca pesan yang sudah dienkripsi. Saat ini enkripsi telah digunakan pada sistem secara luas, seperti Internet e-commerce, jaringan Telepon bergerak dan ATM pada bank

Enkripsi secara umum terdiri dari ***plaintext*** (Informasi yang asli), ***ciphertext*** (bentuk yang sudah dienkripsi), ***key*** (parameter dari sebagian dari informasi utama). biasanya proses

enkripsi menggunakan algoritma khusus, mulai dari yang sederhana sampai algoritma yang sangat rumit untuk menyembunyikan pesan atau sumber informasi, salah satu algoritma enkripsi klasik yang biasa digunakan yaitu **Cipher**. Ada berbagai macam jenis — jenis enkripsi cipher diantaranya seperti Caesar Cipher, Vigènere Cipher, Autokey Cipher, Reverse Cipher, Zig-Zag Cipher, dan Lainnya.

**Perbedaan Hash dan Enkripsi**

Perbedaan hash dengan enkripsi adalah hash tidak memiliki kunci atau dekriptor untuk mengembalikan suatu informasi yang sudah teracak. Maka dari itu, biasanya hash digunakan pengaman password supaya seorang tidak bisa mengetahuinya.

**Hash Pada CodeIgniter**

Pada CodeIgniter sendiri hash yang digunakan adalah Bcrypt. **Bcrypt** merupakan fungsi hashing kata sandi yang dirancang oleh dua orang peneliti keamanan komputer Niels Provos dan David Mazières, cipher Blowfish adalah dasar pembuatan bcrypt, dan disajikan di USENIX pada tahun 1999. bcrypt dapat melindungi dari serangan rainbow table dengan mengunakan salt, selain itu, bcrypt adalah fungsi adaptif: seiring waktu, jumlah iterasi dapat ditingkatkan untuk membuatnya lebih lambat, sehingga tetap aman terhadap serangan pencarian brute-force bahkan dengan meningkatnya daya komputasi.
Contohnya adalah hasil hash dari 23 adalah :
$2y$10$Dh0ANLbc2FBbGXIalsS2Pua/jzebRlImtcQir9x/DjQpwOJgzg0W2

**Cara Kerja Hash pada CodeIgniter**

Setelah melakukan register maka password akan ter-hash lalu kode abstrak tersebut disimpan kedalam database , dan ketika user melakukan login , akan dipanggil fungsi password verify yang membalikkan kode abstrak tersebut menjadi password semula ketika sign up (password si user) dan dibandingkan apakah sama atau tidak dengan input type ketika log in.