TUGAS KEAMANAN INFORMASI DAN JARINGAN

HASH FUNCTION

Disusun Oleh:

Nama : Muhammad Haikal Fikri As'ad

NIM : 1203210065

Kelas : IF-01-02

PROGRAM STUDI S1 INFORMATIKA

FAKULTAS TEKNOLOGI INFORMASI DAN BISNIS

INSTITUT TEKNOLOGI TELKOM SURABAYA

2023

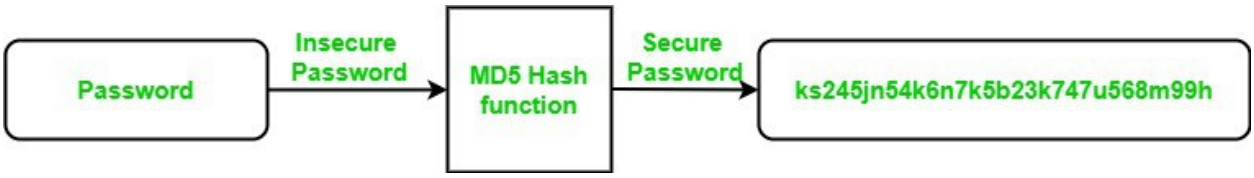
HASH FUNCTION

Hash function adalah fungsi matematis yang mengambil input (atau 'pesan') dan mengembalikan nilai hash, yang biasanya berupa nilai tetap yang memiliki panjang tetap. Fungsi ini dirancang untuk menghasilkan nilai hash yang unik atau seakan-akan acak untuk setiap input yang berbeda. Hash function memiliki beberapa karakteristik penting:

- Deterministik: Fungsi hash harus menghasilkan nilai hash yang sama untuk input yang sama setiap kali dijalankan. Ini berarti hasilnya dapat diprediksi jika inputnya diketahui.
- Efisien: Fungsi hash seharusnya dapat dihitung dengan cepat, terlepas dari ukuran atau kompleksitas input.
- Tidak terbalik (One-way): Sulit untuk mengembalikan input asli dari nilai hash. Idealnya, tidak mungkin melakukan inversi pada nilai hash untuk mendapatkan kembali pesan asli.
- Tidak ada kolisi: Dua input yang berbeda seharusnya tidak menghasilkan nilai hash yang sama. Ini menjaga keunikan dan integritas hash.
- Avalanche Effect: Perubahan kecil pada input seharusnya menyebabkan perubahan besar pada nilai hash. Ini berarti sedikit perubahan pada pesan seharusnya menghasilkan nilai hash yang sangat berbeda.

Fungsi hash digunakan dalam berbagai konteks, termasuk keamanan kriptografi, integritas data, pencocokan password, dan pembuatan checksum. Beberapa algoritma hash yang umum digunakan meliputi MD5, SHA-1, SHA-256, dan SHA-3. Dalam keamanan modern, disarankan untuk menggunakan algoritma hash yang aman, seperti SHA-256 atau SHA-3, karena algoritma hash yang lebih tua seperti MD5 dan SHA-1 telah terbukti rentan terhadap serangan kriptoanalisis.

Algoritma MD5 :



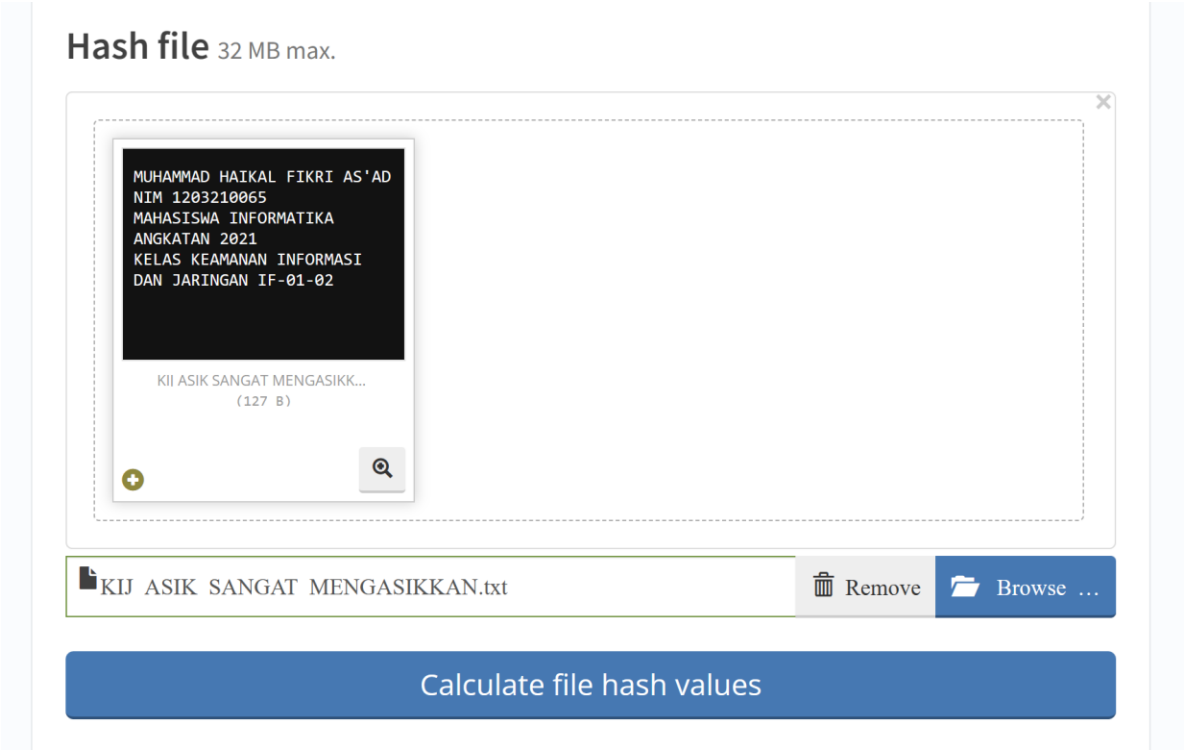
Langkah-langkah :

1. inisialisasi Variabel:
   Empat variabel 32-bit diinisialisasi dengan nilai awal tertentu. Variabel ini akan menyimpan intermediate hash values selama proses.
2. Padding Pesan:
   Pesan yang akan di-hash di-padding sehingga panjangnya menjadi kelipatan 512-bit. Padding dilakukan dengan menambahkan 1 bit setelah pesan, diikuti dengan nol hingga panjang pesan setelah padding menjadi 64 bit kurang dari kelipatan 512-bit.
3. Pengolahan Blok:
   Pesan yang telah di-padding dibagi menjadi blok-blok 512-bit. Setiap blok diolah satu per satu.Setiap blok dipecah menjadi 16 blok 32-bit.

4. Inisialisasi Hash:
   Setiap blok pesan diolah menggunakan fungsi-fungsi logika, pergeseran bit, dan operasi biner dengan variabel hash dari blok sebelumnya.
5. Iterasi:
   Ada 64 iterasi yang dilakukan untuk setiap blok pesan.Fungsi-fungsi logika dan aritmatika diterapkan pada blok sebelumnya dan output dari iterasi sebelumnya.
6. Hasil Akhir:
   Setelah semua blok pesan diolah, hasil akhir dari iterasi tersebut adalah hash nilai yang akan digunakan sebagai representasi unik dari pesan asli.

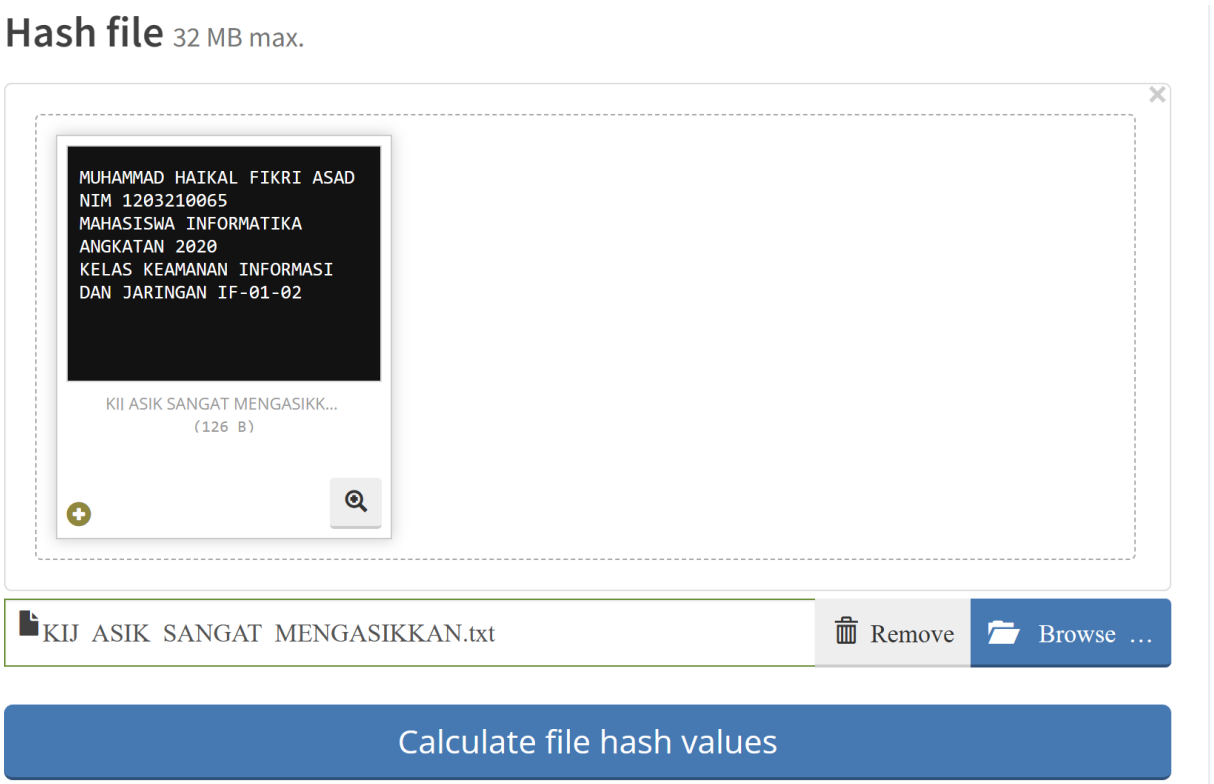
Percobaan mencari nilai hash menggunakan MD5 dengan menggunakan tools yang merupakan web,berikut link WEB nya Hash Calculator Online — String & File Hash Generator (pelock.com) :

- Percobaan 1

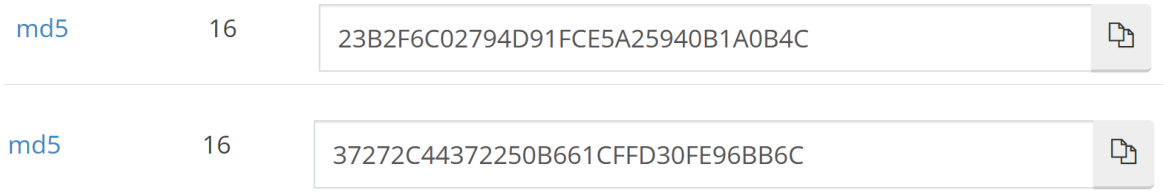


md5	16	23B2F6C02794D91FCE5A25940B1A0B4C

- Percobaan 2
  Pada percobaan 2,saya mengganti isi pesan yang tadinya AS'AD menjadi ASAD dan Angkatan saya ganti menjadi 2020



Perbandingan MD5 1 dan MD5 2



Menandakan bahwa MD5 1 tidak sama dengan MD5 2