

BAB I

PENDAHULUAN

1.1. Latar Belakang

Keamanan suatu data menjadi sangat penting saat sudah berkaitan dengan data yang sangat rahasia. Karena jika sampai dapat diretas atau diketahui oleh orang lain, data yang ada dapat disalahgunakan. Dalam meningkatkan suatu keamanan data, dalam dunia teknologi berkembang sebuah ilmu yakni kriptografi.

Kriptografi adalah ilmu yang mempelajari bagaimana membuat suatu pesan yang dikirim pengirim dapat disampaikan kepada penerima dengan aman. Selain pengertian tersebut terdapat pula pengertian ilmu yang mempelajari teknik-teknik matematika yang berhubungan dengan aspek keamanan informasi seperti kerahasiaan data, keabsahan data, integritas data, serta autentikasi data.

Dalam kriptografi memuat ilmu lain yakni hash. Hash memiliki arti memenggal lalu menggabungkan. Adapun proses hash dikenal sebagai hashing. Hashing seringkali digunakan sebagai metode pencarian suatu data dan menyimpannya dalam memori[1][2]. Namun seiring berjalannya waktu, karena kemampuan hashing mengubah suatu data menjadi string yang merepresentasikan data tersebut, akhirnya dikembangkanlah hashing untuk kriptografi.

Fungsi hash yang dikembangkan untuk kriptografi sudah cukup beragam. Beberapa di antaranya adalah SHA256 dan MD5. Kedua fungsi tersebut umum digunakan dalam kasus kriptografi untuk melakukan pengamanan data. Maka dari itu, masalah yang akan diangkat adalah bagaimana kedua fungsi hash tersebut mampu mengubah data inputan menjadi nilai hash yang menjadi representasi dari data agar tidak dapat dengan mudah diretas atau diketahui oleh orang lain.

1.2. Rumusan Masalah

Dari latar belakang masalah yang dipaparkan, maka dapat dirumuskan masalah yang akan diangkat pada penelitian ini adalah bagaimana cara mengamankan file gambar dan teks menggunakan fungsi hash MD5 dan SHA256.

1.3. Maksud dan Tujuan

Adapun maksud pada penelitian ini adalah:

1. Bagaimana implementasi fungsi hash MD5 dan SHA256 pada file gambar dan teks?
2. Apakah fungsi hash MD5 dan SHA256 dapat melakukan proses hashing pada file gambar dan teks?

Sedangkan tujuan penelitian ini adalah:

1. Menghasilkan program yang mampu melakukan fungsi hash MD5 dan SHA256 pada file gambar dan teks,

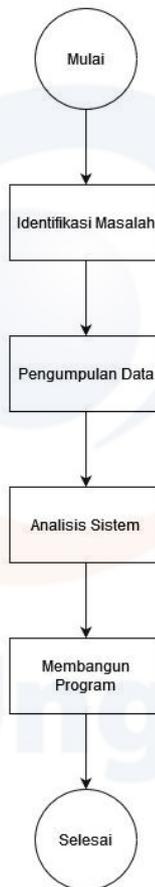
2. Melihat keluaran dari proses hashing yang dilakukan pada file gambar dan teks menggunakan fungsi hash MD5 dan SHA256

1.4. Batasan Masalah

Adapun batasan masalah yang diterapkan pada penelitian ini adalah:

1. Program hanya akan melakukan proses hashing MD5 dan SHA256,
2. Data masukan berupa file gambar dengan format .jpg, .png, ataupun .jpeg serta file teks dengan format .txt
3. Program dibuat menggunakan bahasa pemrograman Python

1.5. Metodologi Penelitian



Gambar 1 Metodologi Penelitian

1. Identifikasi Masalah

Tahap Identifikasi Masalah, merupakan tahap awal penelitian dimana pada proses ini dilakukan pengamatan terhadap penelitian sebelumnya supaya masalah dapat diukur (measurable).

2. Metode Pengumpulan Data

Untuk metode pengumpulan data yang dilakukan, antara lain:

1. Data Primer, yaitu data citra yang akan dikumpulkan dan bersifat baru.
2. Data Sekunder, yaitu data citra yang telah digunakan oleh penelitian sebelumnya atau data citra yang sudah ada dan disediakan secara *open-source*.

3. Analisis Sistem

Pada tahap ini metode yang digunakan akan dianalisis. Metode yang digunakan dalam pembangunan sistem pada penelitian ini memiliki beberapa tahapan yaitu masukan (*input*), proses, dan keluaran (*output*)

4. Membangun Program

Setelah sistem selesai dianalisa pada tahapan sebelumnya, pada tahapan ini program akan mulai dibangun. Program dibangun menggunakan bahasa pemrograman Python.

5. Kesimpulan dan Saran

Menuliskan kesimpulan dari pengamatan dan analisa yang telah dilakukan termasuk juga memberikan saran-saran yang diperlukan.

1.6. Sistematika Penulisan

Sistematika penulisan pada penelitian yang akan dibuat sebagai berikut

BAB 1 PENDAHULUAN

Pada Bab 1 akan diisi dengan Latar Belakang, Maksud dan Tujuan, Identifikasi Masalah, Batasan Masalah, dan Sistematika Penulisan.

BAB 2 LANDASAN TEORI

Pada Bab 2 akan diisi dengan landasan teori hash, kriptografi, dan penelitian terkait..

BAB 3 ANALISIS SISTEM

Pada Bab 3 akan diisi dengan analisis sistem.

BAB 4 PENGUJIAN DAN PEMBAHASAN

Pada Bab 4 akan diisi dengan Implementasi beserta dengan pengujiannya.

BAB 5 KESIMPULAN DAN SARAN

Pada Bab 5 akan diisi dengan kesimpulan penelitian dan saran.