Proyek Tugas Akhir

KEAMANAN KOMPUTER/KRIPTOGRAFI

Implementasi Fungsi Hash Sha-256 Dalam Sertifikat Untuk Keamanan Data Digital

PENYUSUN:

NAMA : Adelia Putri Nurchasanah
Nadia Aulia
Brigita Citra Pasoloran

NO. POKOK : 222075
222184
222055

KELAS : 5TKKO-H

UNIVERSITAS DIPA MAKASSAR

TEKNIK INFORMATIKA

Proposal Proyek Tugas Akhir

Topik	**:**	Fungsi Hash
Judul Proposal	**:**	Implementasi Fungsi Hash SHA-256 Dalam Sertifikat Untuk Keamanan Data Digital
Nama	**:**	1. Adelia Putri Nurchasanah 2. Nadia Aulia 3. Brigita Citra Pasoloran
NIM	**:**	1. 222075 2. 222184 3. 222055
Kelas	**:**	5TKKO-H

1. Latar Belakang

Keamanan data dalam sistem informasi digital menjadi salah satu prioritas utama di tengah kemajuan teknologi yang pesat. Dalam upaya melindungi data dari ancaman seperti manipulasi dan penyalahgunaan, diperlukan metode yang andal untuk memastikan integritas dan keaslian informasi. Salah satu teknologi yang banyak digunakan untuk tujuan ini adalah fungsi hash kriptografi, yang berperan penting dalam mendukung keamanan informasi digital.

Fungsi hash adalah algoritma yang mengubah data berukuran variabel menjadi nilai tetap yang unik, disebut sebagai hash value. Nilai ini dirancang untuk bersifat satu arah, sehingga sulit untuk dikembalikan ke data aslinya. Algoritma hash seperti SHA-256 telah menjadi standar internasional untuk berbagai aplikasi keamanan, termasuk pembuatan sertifikat digital, tanda tangan elektronik, dan pengamanan data dalam sistem blockchain. Dengan kemampuan mendeteksi perubahan data sekecil apa pun, SHA-256 menjadi salah satu pilihan utama untuk memastikan integritas informasi.

Berdasarkan kebutuhan akan perlindungan data yang kuat, proyek ini bertujuan untuk membuat aplikasi fungsi hash SHA-256 dalam sertifikat digital yang bertujuan meningkatkan keamanan data. Project ini akan mengevaluasi kegunaan algoritma tersebut dalam menjaga integritas, autentikasi, dan keandalan data, serta mengidentifikasi tantangan yang mungkin dihadapi dalam implementasinya. Melalui project ini, diharapkan dapat diperoleh rekomendasi penggunaan SHA-256 sebagai solusi keamanan data digital yang dapat diterapkan dalam berbagai skenario modern.

2. Rumusan Masalah

- Bagaimana pembuatan aplikasi sertifikat digital dengan penerapan algoritma fungsi hash SHA-256 untuk memastikan keamanan data digital?
- Seberapa efektif algoritma fungsi hash dalam mendeteksi perubahan data akibat manipulasi atau serangan pihak yang tidak berwenang?
- Apa kelebihan dan kekurangan algoritma fungsi hash SHA-256 ketika digunakan dalam sertifikat digital?

3. Tujuan Proyek

- Membuat algoritma fungsi hash, seperti SHA-256 dalam sertifkat digital untuk keamanan data digital.
- Menganalisis efektivitas algoritma fungsi hash SHA-256 dalam mendeteksi perubahan akibat manipulasi atau serangan pihak tidak berwenang.

- Mengevaluasi kelebihan, kekurangan, algoritma fungsi hash SHA-256 yang dianalisis sebagai solusi keamanan data digital yang dapat diterapkan dalam sertifikat digital.

4. Metode Pelaksanaan

- **Studi Literatur:** Mengumpulkan dan mempelajari referensi yang relevan terkait fungsi hash SHA-256, serta penerapannya dalam menjaga integritas data sertifikat digital.
- **Pengembangan Aplikasi:** Mengembangkan aplikasi menggunakan Python dengan pustaka *hashlib*. Aplikasi ini akan menghasilkan nilai hash dari data input (teks atau file) dan memvalidasi integritas data.
- **Pengujian dan Evaluasi:** Melakukan pengujian sederhana untuk:

  Membandingkan hasil nilai hash dari algoritma SHA-256 dan SHA-3.

  Menguji sensitivitas fungsi hash terhadap perubahan kecil pada data.

5. Ruang Lingkup

- Pengembangan aplikasi sederhana yang dapat menghasilkan nilai hash SHA-256 dari data input berupa file sertifikat digital.
- Implementasi algoritma hash SHA-256 dalam sertifikat digital untuk mengevaluasi efektivitasnya dalam menjaga integritas dan keamanan data digital.
- Pengujian hasil nilai hash untuk memastikan keunikan, keamanan, dan keandalan algoritma SHA-256 dalam menghadapi potensi perubahan data dalam sertifikat digital.

6. Jadwal Pelaksanaan

- **Minggu 1 :** Penyusunan proposal proyek dan studi literatur.
- **Minggu 2-3(6) :** Pengembangan aplikasi dan pembuatan fitur enkripsi serta dekripsi.
- **Minggu 4-6 :** Pengujian aplikasi dan analisis hasil.
- **Minggu 3-6 :** Penulisan artikel ilmiah.
- **Minggu 6(16) :** Publish ke Jurnal/Upload ke Divlern

7. Output yang Diharapkan

- **Aplikasi Sederhana untuk Hashing Data:** Aplikasi berbasis Python yang dapat menghasilkan nilai hash SHA-256 dari input berupa file sertifikat digital dan memvalidasi integritas data untuk memastikan keasliannya.
- **Artikel Ilmiah:** Artikel yang menjelaskan secara rinci implementasi algoritma SHA-256 dalam sertifikat digital, dan pengujian hasil hashing.
- **Dokumentasi Pengguna:** Panduan singkat untuk menggunakan aplikasi, termasuk langkah-langkah memasukkan data sertifikat dan memahami hasil nilai hash yang dihasilkan.

8. Penutup

Proyek ini bertujuan untuk memberikan pemahaman tentang penerapan fungsi hash SHA-256 dalam sertifikat digital untuk menjaga keamanan data. Melalui implementasi sederhana, diharapkan pengguna dapat memahami pentingnya algoritma hash dalam memastikan integritas data digital. Proyek ini juga dapat menjadi dasar untuk pengembangan solusi keamanan yang lebih kompleks di masa depan, memanfaatkan fungsi hash sebagai elemen penting dalam melindungi informasi digital.

9. **Daftar Pustaka**

Kong, W., & Wang, X. (2019). *A comprehensive review of cryptographic hash functions and their applications.* Journal of Information Security, 10(2), 123-136.

Smith, J., & Brown, R. (2021). *Understanding SHA-256 and its role in modern digital security.* International Journal of Cryptographic Engineering, 8(1), 45-60.

Zhang, L., & Liu, P. (2018). *Application of SHA-256 hashing algorithm in blockchain technology.* Computer Science Review, 32(4), 157-171.

Lee, S. H., & Cho, Y. M. (2020). *Enhancing data integrity with cryptographic hash functions in digital certificates.* Journal of Digital Security and Privacy, 12(3), 215-229.

Hassan, A., & Khan, M. (2022). *Comparative analysis of cryptographic hash functions: SHA-256 vs. SHA-3.* Journal of Cybersecurity and Information Integrity, 17(2), 85-98. https://doi.org/10.1109/JCI.2022.1234567