ANALISIS DAN PERANCANGAN KEAMANAN DATA TEKS MENGGUNAKAN ALGORITMA KRIPTOGRAFI SECURE HASH ALGORITHM

SKRIPSI

Oleh:

Irwan Suhendra

200210013

PROGRAM STUDI TEKNIK INFORMATIKA
FAKULTAS TEKNIK DAN KOMPUTER
UNIVERSITAS PUTERA BATAM

TAHUN 2024

ANALISIS DAN PERANCANGAN KEAMANAN DATA TEKS MENGGUNAKAN ALGORITMA KRIPTOGRAFI SECURE HASH ALGORITHM

SKRIPSI

Untuk memenuhi salah satu syarat
memperoleh gelar Sarjana

Oleh:

Irwan Suhendra

200210013

PROGRAM STUDI TEKNIK INFORMATIKA
FAKULTAS TEKNIK DAN KOMPUTER
UNIVERSITAS PUTERA BATAM
TAHUN 2024

SURAT PERNYATAAN ORISINALITAS

SURAT PERNYATAAN ORISINALITAS

Yang bertanda tangan di bawah ini saya :

Nama : Irwan Suhendra

Npm : 20020013

Fakultas : Teknik dan Komputer

Program Studi : Teknik Informatika

Menyatakan bahwa "**Skripsi**" yang saya buat dengan judul :

Analisis dan Perancangan Keamanan Data Teks Menggunakan Algoritma Kriptografi Secure Hash Algorithm.

Adalah hasil karya sendiri dan bukan bukan " publikasi" dari karya orang lain. Sepengetahuan saya, di dalam naskah Skripsi ini tidak terdapat karya ilmiah atau pendapat yang pernah ditulis atau diterbitkan oleh orang lain, kecuali yang secara tertulis dikutip dalam naskah ini dan disebutkan dalam sumber kutipan dan daftar pustaka.

Apabila ternyata di dalam naskah Skirpsi ini dapat dibuktikan terdapat unsur-unsur PLAGIASI, saya bersedia naskah Skripsi ini digugurkan dan gelar akademik yang saya peroleh dibatalkan, serta diproses sesuai dengan peraturan perundang-undangan yang berlaku.

Demikian surat pernyataan ini saya buat dengan sadar diri dan tanpa ada paksaan dari pihak manapun

Batam, 25 Januari 2024

Irwan Suhendra
200210013

iii

HALAMAN PENGESAHAN

ANALISIS DAN PERANCANGAN KEAMANAN DATA TEKS MENGGUNAKAN ALGORITMA KRIPTOGRAFI SECURE HASH ALGORITHM

SKRIPSI

Untuk memenuhi salah satu syarat memperoleh gelar Sarjana

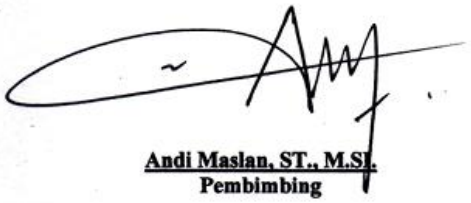
Oleh:

Irwan Suhendra

200210013

Telah disetujui oleh Pembimbing pada tanggal Seperti tertera dibawah ini

Batam, 25 Januari 2024



Andi Maslan, ST., M.SI.
Pembimbing

ABSTRAK

Keamanan data merupakan aspek krusial dalam era digital saat ini, terutama dengan semakin meningkatnya pertukaran informasi melalui jaringan, sehingga keamanan jaringan berupaya untuk mengamankan dari bahaya dan ancaman fisik maupun logis yang dapat mencuri data-data pribadi. Penelitian ini bertujuan untuk menganalisis dan perancangan sistem keamanan data teks dengan memanfaatkan algoritma kriptografi *Secure Hash Algorithm* (SHA) agar meningkatkan tingkat keamanan dan integritas data teks melalui penerapan teknologi kriptografi yang handal. Metode penelitian yang digunakan adalah *Secure Hash Algorithm* (SHA) 256 untuk menganalisis data teks, dan nantinya data teks tersebut akan diolah menggunakan aplikasi *SHA 256* untuk mengetahui cara kerja dan implementasinya pada pengamanan data teks. Hasil untuk cara kerja *SHA* memiliki nilai awal yang sudah ditentukan untuk setiap literasi hash yang dihasilkan dari beberapa bilangan prima, pesan yang akan di-hash dibagi menjadi blok-blok lebih kecil, yang setiap bloknya memiliki Panjang 512-bit dan dilakukan padding agar Panjang teks dapat dibagi 512 yang nantinya untuk setiap blok teks diolah berulang kali sebanyak 64 putaran, setelah semua blok teks diolah, maka nilai hash yang dihasilkan berupa serangkaian bit dengan Panjang tertentu. Hasil untuk Langkah-langkah implementasi *SHA* yang pertama adalah mengambil data teks yang ingin diamankan, kemudian konversi data teks menjadi format *ASCII/Unicode*, jalankan algoritma *SHA* untuk mencari nilai hash, simpan nilai hash kedalam database, kemudian verifikasi keaslian data teks, jalankan algoritma *SHA* pada data tersebut dan bandingkan nilai hash yang dihasilkan dengan nilai hash yang sebelumnya disimpan, jika hasilnya sama, maka data teks tersebut asli. Rekomendasi yang dapat diberikan adalah untuk mendalami dan mengembangkan sisi blockhchain dan meningkatkan Kembali pada aplikasi *SHA 256* dibagian testingnya.

Kata Kunci: Algoritma Kriptografi, Keamanan Data*, Nilai Hash, Secure Hash Algorithm*, Verifikasi Keaslian.

ABSTRACT

Data security is a crucial aspect in the current digital era, especially with the increasing exchange of information over the network, so that network security attempts to protect against physical and logical dangers and threats that can steal personal data. This research aims to analyze and design a text data security system by utilizing the Secure Hash Algorithm (SHA) cryptographic algorithm in order to increase the level of security and integrity of text data through the application of reliable cryptographic technology. The research method used is the Secure Hash Algorithm (SHA) 256 to analyze text data, and later the text data will be processed using the SHA 256 application to find out how it works and its implementation in securing text data. The results for how SHA works have an initial value that has been determined for each hash literacy produced from several prime numbers, the message to be hashed is divided into smaller blocks, each block has a length of 512 bits and padding is done to make the text longer. can be divided by 512 which will then be processed repeatedly for 64 rounds for each text block. After all the text blocks have been processed, the resulting hash value is a series of bits with a certain length. The results for the first SHA implementation steps are to take the text data you want to secure, then convert the text data into ASCII/Unicode format, run the SHA algorithm to find the hash value, save the hash value into the database, then verify the authenticity of the text data, run the SHA algorithm on the data and compare the resulting hash value with the previously stored hash value, if the results are the same, then the text data is genuine. The recommendation that can be given is to explore and develop the blockchain side and improve the SHA 256 application in the testing section.

Keywords: Cryptographic Algorithm, Data Security, Hash Value, Secure Hash Algorithm, Authenticity Verification.

KATA PENGANTAR

Puji syukur saya ucapkan kepada Allah SWT yang telah melimpahkan segala rahmat dan karuniaNya, sehingga penulis dapat menyelesaikan laporan tugas akhir yang merupakan salah satu persyaratan untuk menyelesaikan program studi strata satu (S1) pada Program Studi Teknik Informatika Universitas Putera Batam.

Penulis menyadari bahwa Skripsi in masih jauh dari sempurna, Karena itu, kritik dan saran akan senantiasa penulis terima dengan senang hati. Dengan segala keterbatasan,penulis menyadari pula bahwa skripsi ini takkan terwujud tanpa bantuan, bimbingan, dan dorongan dari berbagai pihak. Untuk itu, dengan segala kerendahan hati, penulis menyampaikan ucapan terima kasih kepada:

1. Ibu Dr. Nur Elfi husda, S.Kom., M.SI selaku Rektor Universitas Putera Batam.
2. Bapak Andi Maslan, S.T., M.SI. selaku Ketua Program Studi Teknik Informatika Universitas Putera Batam dan sekaligus menjadi pembimbing skripsi pada Program Studi Teknik Informatika Universitas Putera Batam.
3. Bapak Ellbert Hutabri, S.Kom., M.Kom selaku pembimbing Akademik pada Program Studi Teknik Informatika Universitas Putera Batam.
4. Bapak Welly Sugianto, S.T., M.M. selaku Dekan pada Program Studi Teknik Informatika Universitas Putera Batam.
5. Seluruh Dosen dan Staff Universitas Putera Batam yang telah memberikan pengetahuan kepada kami selama kuliah.
6. Kedua Orang Tua ayahanda Zulfikar dan ibunda Ernawilis yang tercinta terima kasih atas kasih sayang, kesabaran, serta dukungan dan doa yang begitu banyak di berikan dan ikhlas tanpa pamrih.
7. Teman – teman mahasiswa Teknik Informatika terkhusus kepada Isnaini Hutagalung, Halimah Tuss'adiyah, Elza Maudy Zahra, Winda Syukur, Linda Siregar, Mayana Kris Monika, Yohana Ndoya, Shyntia Rahayu, Dedek Rahmadani, Rizky Amin Febrianto, Ibrani Gaho yang telah memberikan masukan serta saran nya agar penelitian ini bisa sukses.

Semoga Allah SWT membalas kebaikan dan selalu mencurahkan hidayah serta taufik-Nya, Amin.

Batam, 25 Januari 2024

Penulis

Irwan Suhendra

vii

DAFTAR ISI

DAFTAR GAMBAR

DAFTAR TABEL

DAFTAR LAMPIRAN