Terbit *online* pada laman web jurnal : http://ejournal.upbatam.ac.id/index.php/comasiejournal

Jurnal Comasie

ISSN (Online) 2715-6265

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

Irwan Suhendra[1], Andi Maslan[2]

[1]Teknik Informatika, Universitas Putera Batam
[2]Teknik Informatika, Universitas Putera Batam *email*:
pb200210013@upbatam.ac.id

ABSTRACT

Data security is a crucial aspect in today's digital era, especially with the increasing exchange of information over the network, so network security seeks to secure from physical and logical dangers and threats that can steal personal data. This research aims to analyse and design a text data security system by utilising 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 Secure Hash Algorithm (SHA) 256 to analyse text data, and later the text data will be processed using the SHA 256 application to find out how it works and its implementation on securing text data. The results for how SHA works have a predetermined initial value for each hash literacy generated from several prime numbers, the message to be hashed is divided into smaller blocks, each of which has a length of 512 bits and padding is done so that the length of the text can be divided by 512 which later for each text block is processed repeatedly for 64 rounds, after all text blocks are processed, the resulting hash value is a series of bits with a certain length. The results for the SHA implementation steps are first to take the text data to be secured, 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 hash value generated with the hash value previously stored, if the result is the same, then the text data is original. Recommendations that can be given are to explore and develop the blockhchain side and improve the SHA 256 application in the testing section.fritzing.

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

PENDAHULUAN

Perkembangan zaman digital saat ini, peningkatan yang signifikan dalam penerapan teknologi informasi telah menimbulkan tantangan baru terhadap keamanan data. Seiring dengan kemajuan teknologi, perlindungan terhadap data berbentuk teks menjadi semakin vital,

Terbit *online* pada laman web jurnal : http://ejournal.upbatam.ac.id/index.php/comasiejournal

Jurnal Comasie

ISSN (Online) 2715-6265

terutama mengingat adanya informasi rahasia dan data penting seperti data keuangan, identitas, dan komunikasi bisnis yang disimpan dalam format teks.

Perlindungan data teks mencakup upaya untuk mempertahankan data dari ancaman terhadap integritas dan validitas data serta melindunginya dari akses yang tidak diinginkan. Oleh karena itu, diperlukan strategi mutakhir dan efektif untuk menjaga data teks dari potensi bahaya.

Tentu saja, ada kemungkinan individu yang ceroboh akan mendapatkan akses ke informasi pribadi dan sensitif, yang dapat merugikan atau bahkan membahayakan perusahaan dan pengirimnya. Isinya mungkin berubah, sehingga menyebabkan kesalahpahaman di pihak penerima pesan. Selain itu, data yang dicuri dapat hilang atau rusak, sehingga mengakibatkan kerugian finansial yang signifikan.

Teknik kriptografi hash yang aman mengambil peran utama dalam konteks ini. Algoritma ini memastikan integritas data dan tidak memungkinkan pihak yang tidak berkepentingan untuk menguraikannya, sehingga memberikan tingkat keamanan yang tinggi. Untuk menjamin keamanan informasi dalam lingkungan digital yang menjadi lebih rumit, penting untuk menganalisis dan mengembangkan keamanan data teks menggunakan metode kriptografi hash yang aman.

Secure Hash Algorithm adalah serangkaian algoritma fungsi hash kriptografis yang dikembangkan oleh National Institute of Standards and Technology (NIST) di Amerika Serikat. Tujuan utama Secue Hash Algorithm adalah menghasilkan nilai hash yang unik dan sulit untuk diubah kembali dari sejumlah data input. Algoritma ini digunakan secara luas untuk mengamankan integritas data, verifikasi keaslian, dan dalam berbagai protokol keamanan.

Secure Hash Algorithm mempunyai cara kerja yang sangat unik yaitu Secure Hash Algorithm memiliki nilai awal yang sudah ditentukan untuk setiap iterasi hash. Nilainilai ini dihasilkan dari beberapa bilangan prima. Pesan yang akan di-hash dibagi menjadi blok-blok yang lebih kecil. Setiap blok biasanya memiliki panjang 512-bit. Pesan diisi atau dipad dengan bit tambahan agar memiliki panjang yang sesuai dengan aturan algoritma. Padding dilakukan agar panjang pesan dapat dibagi dengan 512. Setiap blok pesan diolah dengan menggunakan variabelvariabel sementara, dan ini dilakukan berulang kali untuk setiap blok. Setiap blok pesan diolah melalui serangkaian putaran. Jumlah putaran bergantung pada versi SHA yang digunakan
(misalnya, SHA-256 memiliki 64 putaran). Fungsi kunci menggabungkan nilai-nilai variabel sementara untuk menghasilkan nilai hash yang baru. Sesudah semua blok pesan diolah, nilai hash akhir dihasilkan. Nilai ini biasanya berupa serangkaian bit dengan panjang tertentu, seperti 256-bit untuk SHA-256. (Komang Aryasa, 2014: 27-66)

Tingkat keamanan yang tinggi dicapai melalui penggunaan berbagai operasi bitwise, operasi logika, dan operasi matematika yang rumit dalam proses SHA. Fitur kriptografi yang lebih mendalam dan berbagai langkah keamanan digunakan dalam implementasi

Terbit *online* pada laman web jurnal : http://ejournal.upbatam.ac.id/index.php/comasiejournal

Jurnal Comasie

ISSN (Online) 2715-6265

aktual SHA untuk menggagalkan upaya kriptanalisistype

KAJIAN TEORI

2.1 Keamanan Jaringan

Keamanan jaringan adalah suatu proses untuk pencegahan dan identifikasi dari aktifitas penggunaan yang tidak sesuai serta dari jaringan komputer tersebut. Selain itu, keamanan jaringan berupaya untuk mengamankan bahaya dan ancaman berupa ancaman fisik dan logis yang dapat mengganggu baik secara langsung maupun tidak langsung. (Amarudin, Faruk Ulum, 2018: 72-75) Dibawah ini adalah 3 konsep umum yang ada di dalam keamanan jaringan.

1. Risk
   Risiko atau tingkat bahaya untuk menunjukkan kemungkinan penyusup dapat menyusup ke jaringan komputer ditunjukkan dengan risiko atau tingkat bahaya.
2. Threat
   Untuk menyampaikan ancaman dari mereka yang mencoba mendapatkan akses tidak sah ke sistem jaringan komputer pengguna.
3. Vulnerability
   Untuk menunjukkan kekuatan dan ketahanan sistem keamanan terhadap potensi ancaman dan bahaya eksternal.

2.2 Keamanan Data

Salah satu komponen penting dari suatu sistem informasi adalah keamanan. Sayangnya, tidak banyak perhatian yang diberikan terhadap kerentanan keamanan ini. Masalah keamanan sering kali menempati urutan kedua atau bahkan terakhir dalam daftar prioritas. Jika masalah keamanan ini memengaruhi fungsionalitas sistem, masalah ini biasanya diminimalkan atau dihilangkan sama sekali. (Yusnita Sari, 2020: 34) Keamanan data mengacu pada menjaga informasi dalam sistem dari akses ilegal, perubahan, atau penghapusan, serta menjaga sistem komputer dari penggunaan atau modifikasi yang tidak sah. (Sari, 2020: 39) Keamanan data dan informasi memiliki empat komponen utama, yaitu

1.Privacy/Confidentiality yaitu yang mengacu pada tindakan yang diambil untuk menamankan keamanan data milik pribadi dari akses yang tidak sah.

2.Integrity yaitu upaya untuk menghambat pihak yang tidak berkepentingan mengubah data atau informasi.

3.Authentication adalah suatu upaya atau teknik untuk memastikan keabsahan data, seperti apakah informasi yang dikirim benar-benar dilihat oleh penerima yang dituju atau apakah server yang menerima layanan tersebut benar-benar tersumber dari server data yang bersangkutan. Ketersediaan sistem dan data (informasi) bila diperlukan berkorelasi dengan ketersediaan data.

2.3 Algoritma

Algoritme adalah teknik berguna yang muncul sebagai kumpulan perintah yang dinyatakan untuk menghitung suatu fungsi. Saat mengatasi suatu masalah, ada persyaratan keadaan awal yang harus dipenuhi sebelum algoritma dijalankan. Untuk semua kondisi awal yang memenuhi persyaratan, algoritma akan selalu berakhir. Diawali dari nilai awal, serangkaian perintah akan dijalankan untuk memproses kondisi yang ditentukan guna menghasilkan keluaran, setelah itu kondisi akhir akan dipastikan. (Sulistiyawati, 2021: 25)

Terbit *online* pada laman web jurnal : http://ejournal.upbatam.ac.id/index.php/comasiejournal

Jurnal Comasie

ISSN (Online) 2715-6265

Algoritme adalah penjelasan langsung tentang logika yang ditulis oleh pengembang perangkat lunak untuk sistem komputer guna meningkatkan efektivitas perangkat lunak dalam mencapai tujuannya dan menghasilkan hasil dari masukan yang diberikan (terkadang nol).

2.4 Kriptografi

Studi tentang penulisan rahasia, atau kriptografi, bertujuan untuk mengkodekan data dan komunikasi sedemikian rupa sehingga dapat didekripsi dan kemudian didekodekan sekali lagi, menjaga isinya tetap tersembunyi dari mata-mata. Kata kriptografi berasal dari kata Yunani kryptos yang berarti tersembunyi. Studi tentang transformasi data, informasi, dan dokumen menjadi bentuk yang unik dan menantang untuk dipahami dikenal sebagai kriptografi. Ini juga dapat dipahami sebagai tulisan terselubung. (Yusfizal, 2019: 29-37).

Enkripsi, juga dikenal sebagai decipherment, adalah proses mengubah teks biasa menjadi teks tersandi; dekripsi, juga dikenal sebagai decipherment, adalah proses mengembalikan ciphertext ke plaintext. Parameter konversi yang dikendalikan oleh satu atau lebih kunci digunakan dalam kriptografi. 2.5 Secure Hash Algorithm (SHA)

SHA merupakan salah satu dari algoritma dari fungsi hash satu-arah(oneway Algorithm) yang dibuatoleh NSA dan dipublikasikan oleh NIST. SHA adalah perpanjangan dari MD5, yang dianggap tidak aman pada tahun 2005 karena kesalahan algoritmik yang menyebabkan kunci publik berbeda menghasilkan intisari pesan yang identik. Secara komputasi sulit bagi metode SHA ini untuk menemukan pesan yang cocok dengan intisari pesan yang disediakan. Dengan demikian, algoritma ini aman. Enam algoritma SHA yang telah dipublikasikan adalah SHA-0, SHA-1, SHA-224, SHA256, SHA-384, dan SHA-512. (Sialahi, 2020: 12)

Berdasarkan hasil penelitian Komang Aryasa (2014) mengatakan bahwa cara kerja algoritma SHA adalah sebagai berikut:

1.Padding: Pesan masukan dibagi menjadi blok-blok dengan ukuran tetap. Sebelum diproses, pesan sering kali diberi bantalan untuk memastikan pesan tersebut sesuai dengan persyaratan ukuran blok. Padding biasanya mencakup 1 bit diikuti dengan serangkaian angka nol dan panjang pesan asli dalam biner. 2.Nilai Hash Awal: Algoritme SHA menggunakan sekumpulan konstanta awal, yang sering disebut sebagai "IV" (Vektor Inisialisasi). IV ini telah ditentukan sebelumnya dan memberikan status awal untuk komputasi hash.

3.Perhitungan Intisari Pesan: Perhitungan hash berlangsung dalam serangkaian putaran. Setiap putaran melibatkan serangkaian fungsi logika dan operasi bitwise, termasuk bitwise AND, OR, XOR, dan bit yang berputar. 4 Komponen utama dari setiap putaran adalah: Ekspansi Pesan: Blok saat ini diperluas menjadi kumpulan kata yang akan digunakan dalam operasi selanjutnya.

5.Fungsi Kompresi: Kata-kata yang diperluas digabungkan dengan nilai hash saat ini dan diproses melalui serangkaian operasi bitwise.

6.Nilai Hash Akhir: Nilai hash yang dihasilkan dari pemrosesan setiap blok diperoleh. Nilai ini adalah string bit dengan panjang tetap, sering kali direpresentasikan sebagai angka heksadesimal. Fungsi hash SHA

Terbit *online* pada laman web jurnal : http://ejournal.upbatam.ac.id/index.php/comasiejournal

Jurnal Comasie

ISSN (Online) 2715-6265

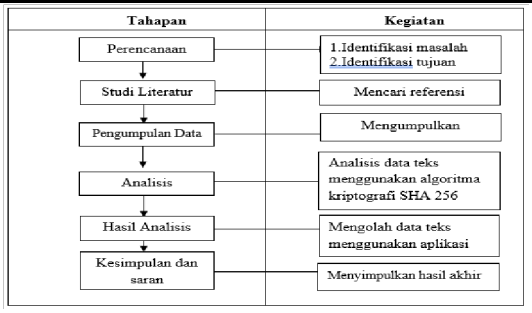
dirancang dengan mempertimbangkan properti tertentu:

1. Deterministik: Untuk input yang sama, fungsi hash akan selalu menghasilkan nilai hash yang sama.
2. Komputasi Cepat: Algoritme SHA dirancang agar efisien secara komputasi sekaligus memberikan keamanan yang kuat.
3. Resistensi Preimage: Mengingat nilai hash, secara komputasi tidak mungkin untuk menentukan input asli.
4. Ketahanan Tabrakan: Tidak mungkin menemukan dua masukan terpisah yang menghasilkan nilai hash yang sama secara komputasi.
5. Efek Longsoran: Perubahan kecil pada input akan menghasilkan nilai hash yang berbeda secara signifikan.

SHA-1, SHA-256, SHA-384, SHA-512, dan varian lainnya merupakan bagian darii keluarga SHA. Meskipun SHA-1 banyak digunakan di masa lalu, namun kini dianggap lemah karena kerentanannya, dan SHA-256 serta variannya lebih aman dan umum digunakan untuk berbagai tujuan kriptografi, seperti tanda tangan digital dan verifikasi integritas data.
(Aryasa, 2014: 27-66)

METODE PENELITIAN

3.1 Desain Penelitian



Gambar 3. 1 desain penelitian
(Sumber: Data Penelitian, 2023)

Berdasarkan tabel langkah-langkah penelitian di atas, maka penjelasannya sebagai berikut:

1. Perencanaan

Langkah pertama dalam mencapai suatu tujuan atau pencapaian adalah perencanaan, yang pada tahap ini berupaya melakukan persiapan terhadap tujuan dan bentuk permasalahan. Tahap ini akan melibatkan beberapa langkah, yang pertama adalah mengidentifikasi masalah yang ingin ditangani, tujuan, dan sejauh mana diskusi:

a. Menentukan masalah Pada Dengan menggunakan algoritma kriptografi Secure Hash Algorithm 2, peneliti akan mengidentifikasi kelemahan pada desain keamanan data teks pada saat ini. Peneliti akan menggunakan masalah ini sebagai topik penelitian. b. Menentukan tujuan Untuk meningkatkan keamanan data teks kedepannya, peneliti akan mengidentifikasi tujuan atau solusi dari permasalahan yang ada saat ini dalam perancangan keamanan data teks dengan menggunakan algoritma kriptografi Secure Hash Algorithm 2.

c. Menentukan ruang lingkup Penetapan ruang lingkup akan membantu memastikan bahwa penelitian terfokus dan tidak menyimpang dari pokok

Terbit *online* pada laman web jurnal : http://ejournal.upbatam.ac.id/index.php/comasiejournal

Jurnal Comasie

ISSN (Online) 2715-6265

bahasan. Dimana penelitian ini hanya membahas perancangan keamanan data teks dengan memanfaatkan algoritma kriptografi Secure Hash Algorithm 2.

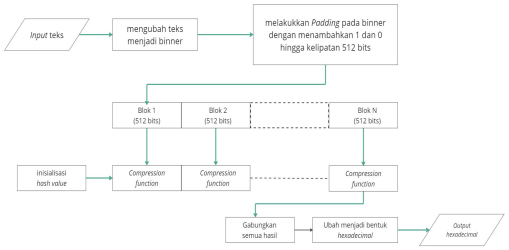
2. Studi literature

Langkah selanjutnya setelah perencanaan adalah studi literatur, dimana peneliti mencari referensi untuk menemukan pengetahuan atau penelitian sebelumnya yang diperlukan. 3. Pengumpulan data Tahap selanjutnya disebut pengumpulan data, dan tujuannya adalah mengumpulkan informasi atau data apa pun yang dibutuhkan peneliti.

4. Analisis

Kemampuan untuk membedah dan menjelaskan sesuatu ke dalam bagianbagian yang dapat dikelola untuk dipahami dikenal sebagai analisis. Analisis dilakukan dengan menggunakan langkahlangkah berikut:

1. Analisis Data
   Analisis data dilakukan untuk megubah hasil penelitian menjadi informasi baru yang berguna untuk mengambil keputusan.
2. Analisis Permasalahan Analisis masalah dilakukan untuk mengidentifikasi permasalahan yang ada dan menentukan solusi dari permasalahan tersebut.
3. Hasil Analisis
   Tahapan ini merupakan proses pengolahan data yang di peroleh dari data perancangan keamanan data teks menggunakan algoritma kriptografi Secure Hash Algorithm 2 (SHA 2).
4. Kesimpulan dan Saran Poin-poin yang telah diselesaikan dari tahap sebelumnya membentuk tahap ini. Rekomendasi ini merupakan perbaikan yang dimaksudkan untuk mengatasi permasalahan yang penting dan bermanfaat bagi penelitian ini. 3.2 Algoritma SHA 256



Gambar 3.2 Algoritma SHA 256

Hash 256, sebagai algoritma pengamanan yang kritis, melibatkan serangkaian proses sistematis yang kompleks. Ini mencakup tahap-tahap esensial yang digunakan oleh sistem untuk mengonversi teks menjadi hash dengan keefisienan dan keamanan yang tinggi. Berikut adalah Algoritma dari SHA 256: Memasukkan teks yang akan dilakukan hash,Mengubah teks menjadi binner,Teks yang dimasukkan diubah menjadi biner berdasarkan nilai desimal yang terkandung dalam kode ASCII,Melakukkan pemadatan biner (Padding)

Setelah itu, dilakukan pemadatan teks (padding),Proses ini melibatkan penambahan angka 1 di akhir blok, diikuti oleh penambahan angka 0 untuk mengisi ruang padding yang diperlukan hingga total bit mencapai 512.,setelah itu, Pengelolahan hasil binner (Compression Function), lalu Menggabungkan hasil dari setiap blok

Setelah dilakukan enkripsi, maka akan menggabungkan hasil enkripsi per blok (512 bit) dalam bentuk binner.Konversi binner menjadi hexadecimal.

Terbit *online* pada laman web jurnal : http://ejournal.upbatam.ac.id/index.php/comasiejournal

Jurnal Comasie

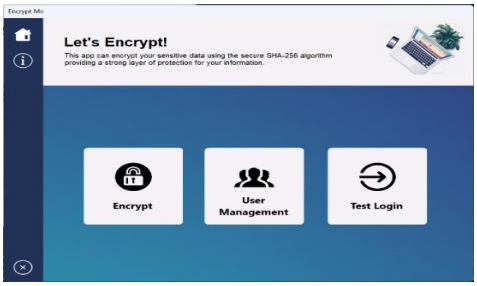
ISSN (Online) 2715-6265

HASIL DAN PEMBAHASAN

4.1 Hasil

Hasil penelitian ini menghasilkan aplikasi desktop "Encrypt Me" dengan implementasi enkripsi SHA-256. Aplikasi ini dibuat dengan tujuan untuk melakukan analisa, menyimpan hasil enkripsi, dan test hasil enkripsi. Fitur yang terdapat pada aplikasi ini yaitu enkripsi teks menjadi hash-256, manajemen user, dan form login yang bertujuan untuk memvalidasi hasil enkripsi.Tampilan antarmuka intuitif membantu pengguna menggunakan fitur enkripsi SHA-256 secara efisien. tampilan dari aplikasi “Encrypt Me”.

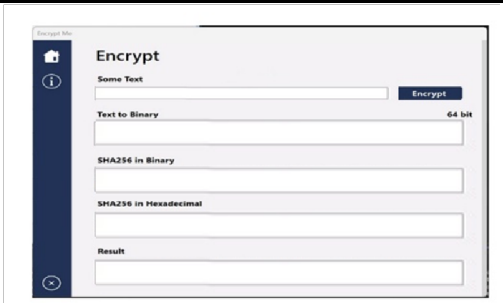
1. Tampilan Halaman Utama



Gambar 4.1 Halaman Utama

Halaman utama aplikasi ditampilkan di atas. Ada 3 tombol dinavigasi bagian Halaman utama aplikasi ditampilkan di atas. Ada 3 tombol dinavigasi bagian kiri terdiri dari tombol untuk ke halaman utama, halaman informasi, dan tombol untuk tutup aplikasi.

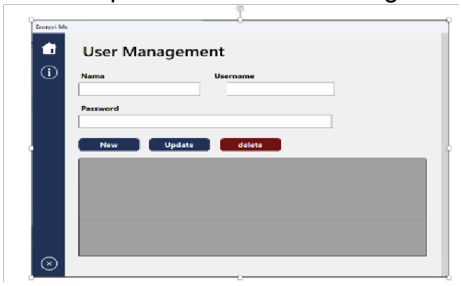
2. Tampilan modul Encrypt



Gambar 4. 2 Halaman Encrypt

Diatas merupakan modul encrypt, didalam modul ini user dapat memasukkan teks yang ingin di enkripsi. Setelah itu user dapat menekan tombol encrypt untuk melakukan enkripsi terhadap teks yang telah dimasukkan. Kemudian system akan memproses teks tersebut.

3. Tampilan modul User Management



Gambar 4. 3 Halaman Registrasi

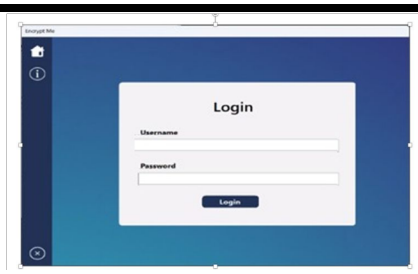
Diatas merupakan tampilan dari modul user management yang digunakan untuk melakukan managemen user yaitu tambah, edit, dan hapus. Didalam modul ini terlihat kolom password yaitu hasil enkripsi yang telah disimpan oleh system.

4. Tampilan Halaman Login

Terbit *online* pada laman web jurnal : http://ejournal.upbatam.ac.id/index.php/comasiejournal

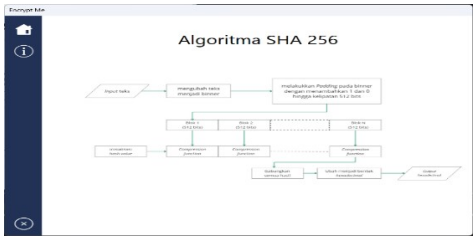
Jurnal Comasie

ISSN (Online) 2715-6265



Gambar 4. 4 Halaman Login

Gambar diatas merupakan tampilan dari modul user management yang digunakan untuk melakukan managemen user yaitu tambah, edit, dan hapus. Didalam modul ini teTampilan halaman login ditampilkan di atas yang digunakan untuk melakukan validasi hasil dari enkripsi password.rlihat kolom password yaitu hasil enkripsi yang telah disimpan oleh system. 5. Tampilan Halaman Informasi



Gambar 4.5 Halaman Informasi

Gambar diatas merupakan tampilan halaman informasi mengenai algoritma dari SHA 256.

3.2 Pembahasan

a. Cara kerja algoritma kriptografi Secure Hash Algorithm 2 (SHA 2) dalam mengamankan data teks

SHA-256 dilakukan dengan mengkonversi teks menjadi biner, menambahkan padding, melakukan pengelompokan per blok, menerapkan fungsi hash seperti XOR, Majority, dan Sigma, menggabungkan hasilnya, lalu mengonversi ke dalam bentuk heksadesimal. Secure Hash Algorithm mempunyai cara kerja yang sangat unik yaitu Secure Hash Algorithm memiliki nilai awal yang sudah ditentukan untuk setiap iterasi hash. Nilai-nilai ini dihasilkan dari beberapa bilangan prima. Pesan yang akan di-hash dibagi menjadi blok-blok yang lebih kecil. Setiap blok biasanya memiliki panjang 512-bit. Pesan diisi atau dipad dengan bit tambahan agar memiliki panjang yang sesuai dengan aturan algoritma. Padding dilakukan agar panjang pesan dapat dibagi dengan 512. Setiap blok pesan diolah dengan menggunakan variabel-variabel sementara, dan ini dilakukan berulang kali untuk setiap blok. Setiap blok pesan diolah melalui serangkaian putaran. Jumlah putaran bergantung pada versi SHA yang digunakan (misalnya, SHA-256 memiliki 64 putaran). Fungsi kunci menggabungkan nilai-nilai variabel sementara untuk menghasilkan nilai hash yang baru. Sesudah semua blok pesan diolah, nilai hash akhir dihasilkan. Nilai ini biasanya berupa serangkaian bit dengan panjang tertentu, seperti 256-bit untuk SHA-256.

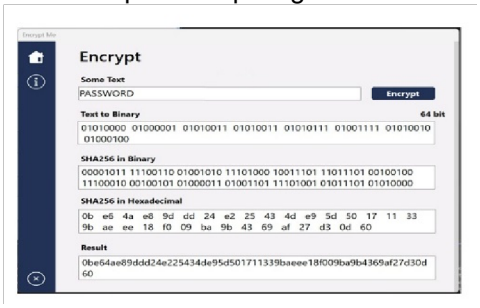
b. Mengimplementasikan algoritma SHA dalam perancangan aplikasi keamanan data teks Implementasi algoritma SHA dapat digunakan dalam perancangan aplikasi keamanan data teks dengan cara menghasilkan nilai hash dari data teks yang ingin diamankan. Berikut adalah langkah-langkah mengimplementasikan algoritma SHA 256 dalam perancangan aplikasi keamanan data teks pada penelituan ini;

Terbit *online* pada laman web jurnal : http://ejournal.upbatam.ac.id/index.php/comasiejournal

Jurnal Comasie

ISSN (Online) 2715-6265

1. Ambil data teks yang ingin diamankan. Pada penelitian ini kita ambil contoh data yaitu " PASSWORD"
2. Kita masukkan "PASSWORD" ini ke dalam aplikasi seperti gambar di bawah



Gambar 4. 6 Implementasi Data Teks

Gambar diatas merupakan proses encrypt, didalam modul ini user dapat memasukkan teks yang ingin di enkripsi seperti contoh kita masukkan "PASSWORD" untuk di encrypt. Setelah itu user dapat menekan tombol encrypt untuk melakukan enkripsi terhadap teks yang telah dimasukkan. Kemudian system akan memproses teks tersebut. Hasil dari enkripsi akan ditampilkan dibawahnya, diawali dengan biner dari teks yang belum dienkripsi, kemudian hasil dari hash 256 dalam bentuk biner, hasil dari hash 256 dalam bentuk hexa decimal dengan spacing, dan hasil dari hash 256 tanpa spacing yang akan disimpan oleh system ke dalam database.

SIMPULAN

Dari dari analisis dan perancangan aplikasi keamanan data teks menggunakan algoritma SHA dan telah dilakukan juga pengujian terhadap aplikasi maka di dapatkan kesimpulan sebagai beriku:

1. Secure Hash Algorithm mempunyai cara kerja yang sangat unik yaitu Secure Hash Algorithm memiliki nilai awal yang sudah ditentukan untuk setiap literasi hash. Nilai-nilai ini dihasilkan dari beberapa bilangan prima. Pesan yang akan di-hash dibagi menjadi blok-blok yang lebih kecil. Setiap blok biasanya memiliki panjang 512-bit. Pesan diisi atau dipad dengan bit tambahan agar memiliki panjang yang sesuai dengan aturan algoritma. Padding dilakukan agar panjang pesan dapat dibagi dengan 512. Setiap blok pesan diolah dengan menggunakan variabel-variabel sementara, dan ini dilakukan berulang kali untuk setiap blok. Setiap blok pesan diolah melalui serangkaian putaran. Jumlah putaran bergantung pada versi SHA yang digunakan (misalnya, SHA-256 memiliki 64putaran). Fungsi kunci menggabungkan nilai-nilai variabel sementara untuk menghasilkan nilai hash yang baru. Sesudah semua blok pesan diolah, nilai hash akhir dihasilkan. Nilai ini biasanya berupa serangkaian bit dengan panjang tertentu, seperti 256-bit untuk SHA-256.
2. langkah-langkah mengimplementasikan algoritma SHA dalam perancangan aplikasi keamanan data teks:

a. Ambil data teks yang ingin diamankan.
b. Konversi data teks menjadi format yang dapat diproses oleh algoritma SHA, seperti ASCII atau Unicode.
c. Jalankan algoritma SHA pada data teks untuk menghasilkan nilai hash.
d. Simpan nilai hash yang dihasilkan ke dalam database atau file terpisah.
e. Saat ingin memverifikasi keaslian data teks, ambil kembali data teks yang ingin diverifikasi dan jalankan algoritma SHA pada data tersebut.
f. Bandingkan nilai hash yang dihasilkan dengan nilai hash yang disimpan sebelumnya. Jika kedua nilai hash

Terbit *online* pada laman web jurnal : http://ejournal.upbatam.ac.id/index.php/comasiejournal

Jurnal Comasie

ISSN (Online) 2715-6265

sama, maka data teks tersebut dapat dipastikan keasliannya.

Dengan mengimplementasikan algoritma SHA dalam perancangan aplikasi keamanan data teks, data teks dapat diamankan dengan lebih baik dan dapat dipastikan keasliannya.

DAFTAR PUSTAKA

Amarudin. (2018). Analisis Dan Implementasi Keamanan Jaringan Pada Mikrotik Router Menggunakan Metode Port Knocking. *Seminar Nasional Sains Dan Teknologi 2018*, 1–7.

Aryasa, K., & Paulus, Y. T. (2015). Implementasi Secure Hash Algorithm-1 Untuk Pengamanan Data Dalam Library Pada Pemrograman Java. *Creative Information Technology Journal*, *1*(1), 57. https://doi.org/10.24076/citec.2013v1i1.10

Sari, I. Y., Muttaqin, Jamaludin, Simarmata, J., Rahman, M. A., Iskandar, A., Pakpahan, A. F., Karim, A., Sugianto, Giap, Y. C., Hazriani, Yendrianof, D., & Manullang, S. O. (2021). *Keamanan Data dan Informasi*.

Silalahi, L., & Sindar, A. (2020). Penerapan Kriptografi Keamanan Data Administrasi Kependudukan Desa Pagar Jati Menggunakan SHA-1. *Jurnal Nasional Komputasi Dan Teknologi Informasi (JNKTI)*, *3*(2), 182–186. https://doi.org/10.32672/jnkti.v3i2.2413

Sulistiyawati, A., & Supriyanto, E. (2021). Implementasi Algoritma K-means Clustring dalam Penetuan Siswa Kelas Unggulan. *Jurnal Tekno Kompak*, *15*(2), 25. https://doi.org/10.33365/jtk.v15i2.1162

Sutejo, S. (2021). Implementasi Algoritma Kriptografi Rsa (Rivest Shamir Adleman) Untuk Keamanan Data Rekam Medis Pasien. *INTECOMS: Journal of Information Technology and Computer Science*, *4*(1), 104–114. https://doi.org/10.31539/intecoms.v4i1.2437

Terbit *online* pada laman web jurnal : http://ejournal.upbatam.ac.id/index.php/comasiejournal

Jurnal Comasie

ISSN (Online) 2715-6265

	**Biodata** Penulis pertama, Irwan Suhendra, merupakan mahasiswa Prodi Teknik Informatika Universitas Putera Batam.
	**Biodata** Penulis kedua Andi Maslan,ST.,M.SI., , merupakan kaprodi Prodi Teknik Informatika Universitas Putera Batam Informasi Universitas Putera Batam. Penulis banyak berkecimpung di bidang IT.