BAB I

PENDAHULUAN

1.1 Latar Belakang

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, 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. Untuk menjaga informasi dan data tetap aman dan sulit dibaca, keamanan data sangatlah penting. Oleh karena itu, informasi ini harus dirahasiakan. Data yang dicuri berbahaya jika orang yang ceroboh membaca informasi pribadi dan penting. Dalam dunia teknologi informasi dan komunikas,

khususnya dalam pertukaran data atau pengiriman informasi kepada penerima, timbul pertanyaan apakah data yang diterima sesuai dengan isi informasi yang dikirimkan oleh pengirim sebenarnya dan apakah informasi yang dikirimkan sesuai dengan isi informasi yang dikirimkan. akurat seperti yang dikirim oleh pengirim sebenarnya. (Zulham et al., 2014).

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. 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* (Aryasa & Paulus, 2015).

Metode *Secure Hash algorithm* adalah fungsi hash kriptografi data yang melakukan transformasi data menggunakan fungsi hash. Metode ini digunakan untuk pengamanan data dan masih banyak lagi.

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 aktual *SHA* untuk menggagalkan upaya kriptanalisis.

Tujuan dari penelitian ini untuk menciptakan sistem yang praktis dan efektif untuk menghasilkan keamanan teks tersebut sekaligus mengkaji potensi keamanan teknik kriptografi *hash* aman dalam melindungi data teks.

Penelitian ini diharapkan dapat membantu secara signifikan dalam mengatasi masalah keamanan data di era digital saat ini dengan berfokus pada pentingnya keamanan data teks dan relevansinya dengan teknik kriptografi *hash* yang aman. Berdasarkan penjelasan yang ada di atas, maka peneliti tertarik untuk melakukan

penelitian terkait **"Analisis dan Perancangan Keamanan Data Teks Menggunakan Algoritma Kriptografi Secure Hash Algorithm"**

1.2 Identifikasi Masalah

Penelitian ini memaparkan beberapa permasalahan yang ditemukan, antara lain:

1. Pentingnya keamanan data teks diera digital dimana terdapat banyak akses perlindungan data teks yang tidak sah serta perubahan secara ilegal.
2. Karena data digital sangat penting, maka harus didistribusikan atau disimpan dengan keamanan yang memadai.

1.3 Batasan Masalah

Batasan masalah dalam penelitian ditetapkan sebagai berikut:

1. Hanya membahas tentang analisis dan perancangan keamanan data teks menggunaka algoritma *kriptografi Secure Hash Algorithm 256 (SHA 256).*
2. Fokus penelitian ini terbatas pada data keamanan teks, yang mencakup bentuk teks biasa.
3. Algoritma yang digunakan dalam keamanan teks data dalam penelitian ini hanya *Algoritma Secure Hash Algorithm 256 (SHA 256).*

1.4 Rumusan Masalah

Berikut rumusan masalah yang didapat sesuai dengan identifikasi masalah yang telah dijelaskan sebelumnya:

1. Bagaimana cara kerja algoritma kriptografi *Secure Hash Algorithm 256 (SHA 256)* dalam mengamankan data teks ?

2. Bagaiamana mengimplementasikan dan pengujian algoritma *SHA 256* dalam perancangan aplikasi keamanan data teks ?

1.5 Tujuan Penelitian

Adapun tujuan dari penelitian yang dilakukan, yaitu:

1. Untuk mengetahui cara kerja keamanan data teks menggunakan algoritma kriptografi *Secure Hash Algorithm algoritma 256 (SHA 256).*
2. Untuk mengetahui pengimplementasian dan pengujian algoritma *SHA 256* dalam perancangan aplikasi keamanan data teks ?

1.6 Manfaat Penelitian

Berikut beberapa manfaat penelitian:

1.6.1 Manfaat Teoritis

Beberapa manfaat teoritis yaitu sebagai berikut:

1. Bagi penulis

   Dapat memperluas pemahaman, pengetahuan, pengalaman, dan dapat menerapkan atau mempraktekkan ilmu keamanan data yang telah penulis dapatkan selama dibangku kuliah.

1.6.2 Manfaat Praktis

1. Manfaat paraktis yang didapat dari penelitin ini ialah supaya dapat mengamankan data teks pada saat disimpan.