BAB I
PENDAHULUAN

1.1.Latar Belakang Masalah.

Pesatnya perkembangan teknologi informasi dan komunikasi telah memicu munculnya kemajuan teknologi informasi. Teknologi informasi telah menjadi bagian penting dari kehidupan. Teknologi informasi mempunyai keterkaitan yang sangat erat dengan berbagai aspek kehidupan manusia, seperti berkomunikasi dan saling bertukar informasi atau data. Saat ini, internet dianggap sebagai sarana paling dekat bagi masyarakat dalam era digital untuk mengakses informasi dan berkomunikasi. [1]

Dengan kemajuan teknologi informasi, dibutuhkan sistem keamanan yang kuat untuk melindungi kerahasiaan informasi atau data, terutama jika data tersebut berada dalam jaringan komputer yang terhubung dengan jaringan lain. Dengan hal tersebut risiko besar dapat muncul apabila pihak yang tidak berwenang berhasil mengakses informasi yang privasi dan berharga. Oleh karena itu, seluruh lapisan masyarakat harus memperhatikan keamanan sistem informasi untuk menghindari kejahatan siber. Ancaman ini menciptakan risiko yang harus dikelola untuk melindungi aset dari serangan dunia maya. Penggunaan kriptografi pun menjadi sangat penting dalam hal ini. [2]

Terdapat berbagai aplikasi tidak berbayar yang memungkinkan pengguna untuk mengirim dan menerima pesan., namun sayangnya, kebanyakan aplikasi perpesanan ini tidak menghadirkan lapisan keamanan yang memadai pada pesan mereka, yang berarti bahwa privasi pengguna tidak dapat dijamin. Hingga saat ini, aplikasi tersebut belum mampu memastikan privasi antara pengirim dan penerima pesan, karena data yang dikirim berupa pesan dalam format yang dapat dibaca langsung (plain text). Data percakapan yang tersimpan di penyedia layanan berupa plaintext. Hal ini menciptakan celah keamanan pada data percakapan, pihak-pihak yang tidak berwenang untuk menyadap komunikasi antara dua orang. Data yang dikirimkan selama percakapan akan melewati pihak penyadap, sehingga penyadap dapat mengakses seluruh informasi yang ditransmisikan. Oleh karena itu, diperlukan sebuah aplikasi perpesanan yang memiliki fokus pada keamanan, dengan kemampuan untuk mengenkripsi dan mendekripsi pesan untuk menjaga privasi dan keamanan pengguna.

Selain enkripsi dan dekripsi, penulis juga melakukan pengujian Avalanche Effect untuk menentukan persentase perubahan pesan saat enkripsi, dengan membandingkan jumlah bit yang berubah pada ciphertext dengan jumlah bit pada plaintext sebelum enkripsi.

Berdasarkan latar belakang tersebut, Penulis terpikir untuk berkontribusi melalui implementasi algoritma AES dan SHA-256 pada pesan yang ditampilkan oleh pengirim pesan. Dengan mengambil judul "Implementasi Algoritma AES dan SHA256 untuk Pengamanan Akun". Tentu saja tanpa menghilangkan fitur keamanan yang sudah ada pada messenger sebelumnya saat mengirimkan pesan antar pengguna. Sistem ini bertujuan dapat melakuakan enkripsi dan deskripsi aplikasi chat messenger, sehingga semua data yang terdapat dalam pesan akan terjamin kerahasiaanya.

1.2.Identifikasi Masalah

Berdasarkan latar belakang di atas, penulis dapat merumuskan masalah yang akan dibahas dalam tulisan ini, antara lain:

1. Kombinasi algoritma AES dan SHA-256 untuk memperkuat pengamanan password dan pesan pada aplikasi chatting berbasis web
2. Pengujian waktu enkripsi dan dekripsi dari kombinasi algoritma AES dan SHA-256
3. Pengujian Avalanche Effect dalam kombinasi AES dan SHA-256

1.3.Rumusan Masalah

Berdasarkan penjelasan dari latar belakang, rumusan masalah yang didapat ialah, "Bagaimana cara mengimplementasikan kriptografi untuk pengamanan pesan menggunakan algoritmaAES dan SHA-256 pada aplikasi chat messenger"

1.4.Batasan Masalah

Batasan masalah dari penelitian ini adalah:

1. Menggabungkan hanya dua algoritma, yaitu AES dan SHA256.
2. Aplikasi yang akan dibuat nanti merupakan aplikasi berbasis web.
3. Fitur utama aplikasi yang akan dibuat merupakan chatting sesama pengguna.
4. Bahasa pemrograman yang digunakan yaitu:
    a. Javascript dengan framework ReactJS untuk Front End
    b. Golang dengan framework Gin Gonic untuk Back End
5. Aspek yang diuji meliputi:
    a. Waktu dari Proses enkripsi dan dekripsi menggunakan kombinasi algoritma AES dan SHA-256.
    b. Menguji Avalanche Effect dari penggabungan algoritma AES dan SHA-256

1.5.Tujuan dan Manfaat

Tujuan dari tulisan ini adalah untuk membuat dan menerapkan kriptografi dengan algoritma AES dan SHA-256 untuk melindungi data aplikasi chat. Manfaat dari penulisan ini adalah memastikan bahwa orang dapat berkomunikasi di internet dengan aman, terbebas dari aktivitas yang merugikan, sehingga orang yang salah tidak mudah mendapatkan data penting.