BAB I
PENDAHULUAN

1.1 Latar Belakang

Perkembangan teknologi informasi semakin memudahkan penggunanya dalam berkomunikasi melalui bermacam-macam media. Tidak sedikit orang memanfaatkan kemajuan teknologi informasi untuk berkomunikasi dengan keluarga, teman, bahkan hingga dosen. Informasi dan data dapat dengan mudah diproses melalui jaringan komputer. Keutuhan suatu sistem merupakan sesuatu yang sangat penting. Hal ini tentu saja menimbulkan resiko jika ada pelaku kejahatan dunia maya yang mencoba untuk mencari celah keamanan untuk mendeteksi dan memanipulasi pesan (Azizah, 2020).

Dalam pengamanan data pesan nantinya ditentukan oleh sulitnya menghitung logaritma diskrit semakin sulit perhitungan matematika yang dibuat maka semakin pula untuk memecahkankan perhitungannya. Hal ini tentu meminimalkan seseorang atau penyadap mendapatkan isi data tersebut. Pertukaran kunci *Diffie-Hellman* adalah metode enkripsi yang dimana membangkitkan sebuah angka ke dalam kekuatan tertentu untuk menghasilkan kunci deskripsi.

Sistem kriptografi juga membutuhkan sebuah wadah untuk menampung setiap data-data aplikasi. Wadah yang memungkinkan kita untuk membuat, menguji dan menerapkan aplikasi dengan cepat. Kontainer memungkinkan pengembang untuk mengemas aplikasi dengan semua bagian yang dibutuhkannya, seperti pustaka dan dependensi lainnya, dan menerapkannya sebagai satu paket. Dengan demikian, berkat wadahnya, pengembang dapat yakin bahwa aplikasi akan berjalan di mesin lainnya terlepas dari pengaturan khusus yang mungkin dimiliki mesin yang mungkin berbeda dari mesin yang digunakan untuk menulis dan menguji kode.

Berdasarkan uraian diatas, maka peneliti tertarik mengamankan menggunakan algoritma *Diffie-Huffman* sebagai metode pertukaran kunci. Peneliti juga tertarik menggunakan teknologi kontainer untuk mengisolasikan tiap-tiap data kedalam satu wadah dengan teknologi Docker container.

1.2 Perumusan Masalah

Rumusan masalah yang dapat didefinisikan dalam penelitian ini diantaranya adalah sebagai berikut :

1. Bagaimana mendesainkan sistem kriptografi pengamanan data pesan dengan algoritma *Diffie Hellman* ?
2. Bagaimana mengimplementasikan sistem kriptografi pengamanan data pesan dengan algoritma *Diffie Hellman* dan teknologi *Docker container*?

1.3 Tujuan Penelitian

Tujuan dari penelitian antara lain :

1. Mendesainkan sistem kriptografi menggunakan algoritma *Diffie Hellman*.
2. Mengimplementasikan kriptografi menggunakan algoritma *Diffie Hellman* sebagai metode kriptografi pengamanan data pesan dan teknologi kontainer *Docker* sebagai wadah membuat, menguji dan menerapkan pengamanan data pesan

1.4 Manfaat Penelitian

Manfaat dari penelitian ini antara lain :

1. Data pesan yang telah dibuat lebih aman dengan adanya kriptografi.
2. Kriptografi dapat meminimalisasikan kebocoran data.
3. Menghasilkan perlindungan terhadap integritasi suatu data pesan.

1.5 Batasan Masalah

Berdasarkan latar belakang yang telah diuraikan diatas, maka perlu dibatasi permasalahan dari skripsi ini. Algoritma *Diffie Hellman* membangkitkan sebuah angka kedalam kekuatan tertentu yang digunakan sebagai kunci deskripsi, enkripsi dan berfokus pada pengamanan data pesan.