BAB I
PENDAHULUAN

1.1 Latar Belakang

Kemajuan teknologi dibidang komputer memungkinkan ribuan orang dan komputer diseluruh dunia saling terhubung dalam satu dunia maya yang dikenal sebagai *internet*. Begitu juga ratusan organisasi seperti perusahaan, pemerintah bahkan pribadi, telah menjadikan informasi sebagai aset yang sangat berharga. Hal ini menyebabkan data dan informasi menjadi sangat penting untuk dilindungi dari manipulasi informasi, pencurian informasi dan serangan terhadap informasi yang secara langsung ataupun tidak.

Adapun salah satu cara untuk mengamankan data tersebut yaitu dengan kriptografi. Kriptografi adalah ilmu sekaligus seni untuk menjaga kerahasiaan pesan (data atau informasi) dengan cara menyamarkannya menjadi bentuk tersandi yang tidak mempunyai makna untuk menjaga kerahasiaan data dari manipulasi informasi, pencurian informasi dan serangan terhadap informasi. Pesan yang dirahasiakan dalam kriptografi disebut pesan asli (*plaintext*) dan hasil penyamaran disebut pesan sandi (*chipertext*). Proses penyamaran dari palinteks ke chiperteks disebut enkripsi (dari kata *encryption*) dan proses pembalikan dari *chipertext* menjadi *plaintext* kembali disebut dekripsi (*decryption*). Baik proses enkripsi maupun proses dekripsi melibatkan satu kunci kriptografi.

Pada penelitian ini penulis menerapkan Algoritma Kriptografi *cipher One time pad* (OTP) sebagai teknik kriptografi yang mencakup proses enkripsi dan dekripsi. Kriptografi *One Time Pad* (OTP) merupakan salah satu jenis teknik kriptografi klasik yang menggunakan metode substitusi dengan cara memberikan kunci acak dan jumlahnya sama dengan *plaintext*.

1.2 Perumusan Masalah

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

1. Bagaimana mendesain proses enkripsi dan proses dekripsi dengan algoritma *One time pad*?
2. Bagaimana hasil penerapan algoritma krptografi *One time pad* pada aplikasi keamanan data teks?

1.3 Tujuan Penelitian

Tujuan pembuatan skripsi ini adalah untuk merancang dan membangun aplikasi kriptografi dengan metode *One Time Pad* (OTP) yang dapat melakukan proses enkripsi (mengubah pesan asli menjadi pesan sandi) dan dekripsi (mengubah pesan sandi menjadi pesan asli) sebagai sarana dalam pengamanan data atau informasi untuk menjaga kerahasiaan informasi dari pihak–pihak yang tidak berkepentingan.

1.4 Manfaat Penelitian

Manfaat pembuatan skripsi ini dengan algoritma kriptografi *One Time Pad* dalam keamanan jaringan adalah :

1. Mengurangi resiko dari manipulasi informasi, pencurian informasi dari pihak – pihak yang tidak bertanggung jawab.
2. Perangkat lunak yang dirancang dapat digunakan sebagai *tools* kriptografi pengaman data teks dengan metode *One Time pad*.

1.5 Batasan Masalah

Batasan Masalah dari penelitian dengan algoritma kriptografi *One time Pad* adalah Penelitian ini di fokuskan hanya untuk keaman data teks dalam berformat *txt*. dengan penggunaan huruf kapital Tanda baca yang bisa masuk ke dalam sistem ini adalah yang biasa orang gunakan pada umumnya (titik, koma, tanda seru, tanda pagar, tanda persen, bintang, tanda kurung, sama dengan, tambah, kurang, tanda tanya, koma, garis miring, tanda petik) dan berupa angkan.