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 menjadi sangat penting untuk dilindungi dari manipulasi informasi. Adapun salah satu cara untuk mengamankan data tersebut yaitu dengan *Hill Cipher*.

Kriptografi adalah ilmu untuk menjaga kerahasiaan pesan dengan cara menyamarkannya menjadi bentuk tersandi yang tidak mempunyai makna untuk menjaga kerahasiaan data dari manipulasi informasi. Pesan yang dirahasiakan disebut pesan asli (*plaintext*) dan hasil penyamaran disebut pesan sandi (*chipertext*).

Proses penyamaran *plaintext* ke *chipertext* disebut enkripsi (dari kata *encryption*) proses pembalikan dari *chipertext* menjadi *plaintext* kembali disebut dekripsi (dari kata *decryption*). Baik proses enkripsi maupun proses dekripsi melibatkan satu kunci matriks 3x3. Pada penelitian ini penulis menerapkan *Algoritma Kriptografi Hill Chiper* yang mencakup proses enkripsi dan dekripsi. *Kriptografi Hill Chiper* merupakan salah satu jenis *kriptografi* klasik yang menggunakan metode subtitusi 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 dekripsi dengan algoritma *hill chiper*?
2. Bagaimana hasil penerapan algoritma *kriptografi hill chiper* pada aplikasi keamanan data teks?
3. Data yang didapatkan hanya sampai mencakup kalimat untuk mendapatkan hasil sempurna.

1.3. Tujuan Penelitian

1. Tujuan pembuatan skripsi ini adalah untuk merancang dan membangun aplikasi kriptografi dengan metode *hill chiper*, yang dapat melakukan proses enkripsi (mengubah pesan asli menjadi pesan sandi) dan dekripsi (mengubah pesan sandi menjadi pesan asli).
2. Sebagai sarana dalam pengamatan data atau informasi untuk menjaga kerahasiaan informasi dari pihak-pihak yang tidak berkepentingan.

1.4. Manfaat Penelitian

Manfaat pembuatan skripsi ini dengan algoritma *kriptografi hill chiper* 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 pengamanan data teks dengan metode *hill chiper*.

1.5. Batasan Masalah

Batasan masalah dari penelitian ini adalah:

1. Penggunaan huruf abjad biasa dan kapital, angka, serta beberapa simbol yang terdapat pada keyboard.
2. Jika menggunakan *key* yang berberda maka mendapatkan hasil yang berbeda.
3. Matriks kunci *Hill Cipher* harus *invertible*.