BAB 1
PENDAHULUAN

1.1. Latar Belakang

Dengan semakin pesatnya perkembangan ilmu pengetahuan dan teknologi, sistem *multiuser* sudah sangat memungkinkan dimana suatu informasi dapat dibagikan kepada komputer atau user lain dalam suatu jaringan komputer ataupun jaringan yang lebih luas lagi yaitu internet. Jika dilihat dari isinya, informasi dapat berupa penting atau tidak penting. Bila dilihat dari sifat persebaran atau *privacy*-nya, informasi dapat bersifat rahasia atau tidak rahasia. Informasi penting dan bersifat rahasia ini harus dijaga dari pihak-pihak yang tidak bertanggung jawab baik terhadap pemalsuan, pencurian maupun pengubahan data secara *illegal*. Salah satu cara untuk mempertahankan kerahasiaannya, maka informasi tersebut dijadikan menjadi kode-kode yang tidak dipahami sehingga penyadap akan kesulitan untuk mengetahui isi informasi yang sebenarnya.

Untuk mengatasi permasalahan di atas, salah satu solusi yang dapat diambil adalah dengan cara penyandian atau kriptografi. Dengan cara ini sebuah informasi akan disandikan berdasarkan metode tertentu sehingga orang yang tidak berkepentingan dan tidak memiliki hak akses akan mengalami kesulitan untuk melakukan hal-hal yang tidak diinginkan. Sebaliknya ketika informasi tersebut akan diakses kembali oleh orang yang berhak maka hasil penyandian tersebut kemudian akan dikembalikan ke bentuk semula. Secara umum, algoritma yang digunakan dalam kriptografi dapat terbagi ke dalam dua macam, yaitu algoritma kriptografi klasik dan algoritma kriptografi modern.

Ada dua teknik kriptografi klasik yaitu teknik subtitusi dan teknik transposisi. Salah satu teknik subtitusi yaitu algoritma *vigenere cipher*. *Vigenere cipher* pertama kali dipopulerkan oleh diplomat (sekaligus seorang kriptologis) Prancis, Blaise de Vigenere pada abad 16. Namun pada zaman sekarang ini teknik kriptografi klasik khususnya vigenere cipher tidak dapat menyaingi metode-metode baru yang lebih baik, karena kesederhanaannya.

Oleh karena itu, maka muncul suatu ide untuk membangun sistem keamanan menggunakan metode *vigenere cipher* yang digabungkan dengan permutasi cipher dengan memodifikasi *key*-nya menjadi dinamis pada setiap blok pesan yang sudah dibagi perkata, yang selanjutnya pada laporan ini disebut dengan Aplikasi Kriptografi Teks Viper Dinamis

Kriptografi mempunyai dua bagian yang penting, yaitu enkripsi dan dekripsi. Enkripsi adalah proses dari penyandian pesan asli menjadi pesan yang tidak dapat diartikan seperti aslinya. Untuk dekripsi merupakan proses mengubah pesan dalam suatu bahasa sandi menjadi pesan asli kembali. Pesan asli biasanya disebut plainteks, sedangkan pesan yang sudah disandikan disebut cipherteks.

1.2. Rumusan Masalah

Bagaimana membuat aplikasi kriptografi menggunakan metode kombinasi *vigenere cipher* dan permutasi cipher dengan modifikasi *key* dinamis pada setiap pesan yang sudah dibagi perblok?

1.3. Batasan Masalah

1. Aplikasi kriptografi yang menggunakan metode *Vigenere Cipher*
2. Metode *vigenere cipher* dikombinasikan dengan permutasi cipher dan modifikasi *key* dinamis
3. Jenis huruf yang digunakan pada plainteks sebanyak 94 karakter
4. Informasi yang diamankan adalah teks (*.txt dan *.doc)
5. Pergeseran *key*-nya hanya 26 karakter
6. Aplikasi menggunakan PHP

1.4. Tujuan

Membuat aplikasi kriptografi menggunakan metode *vigenere cipher* yamg dikombinasikan dan permutasi cipher dengan modifikasi *key* dinamis pada setiap pesan yang sudah dibagi perblok.

1.5. Manfaat

Manfaat yang diharapkan dari penerapan aplikasi ini adalah untuk menjaga kerahasiaan informasi yang berupa teks dari orang yang tidak berhak mengakses (menggaransi bahwa data pribadi tetap pribadi).