BAB I

PENDAHULUAN

1.1 Latar Belakang

Kemudahan yang disediakan kemajuan teknologi dalam pengelolaan dokumen secara digital, justru membuat banyak kejahatan di dunia maya, seperti pencurian informasi yang bersifat rahasia. Hal itu dikarenakan keamanan dokumen digital bersifat lemah dan mudah diakses secara legal ataupun ilegal oleh pihak lain. Oleh karena itu, untuk melindungi data atau pesan digital yang bersifat pribadi atau rahasia dibutuhkan teknik penyandian untuk menyamarkan pesan menjadi bentuk lain sehingga pihak yang tidak berhak menerimanya kesulitan untuk mencuri informasi rahasia tersebut.

Kriptografi merupakan salah satu solusi alternatif untuk keamanan data atau pesan digital, yang dapat menyandikan informasi menjadi bentuk lain. Berdasarkan terminologi, kriptografi adalah ilmu dan seni untuk menjaga keamanan pesan ketika pesan dikirim dari suatu tempat ke tempat lain. Secara umum, kriptografi terdiri atas dua bagian utama yaitu bagian enkripsi dan bagian dekripsi. Dalam prosesnya, pengirim dan penerima informasi akan menyepakati sebuah kunci untuk melakukan proses enkripsi dan proses dekripsi. Pengirim akan mengubah pesan berupa informasi (*plaintext*) menjadi pesan dengan bentuk lain yang sulit dipahami (*ciphertext*) dengan menggunakan kunci tersebut. Proses itu disebut enkripsi. Selanjutnya dekripsi adalah mengembalikan pesan yang sulit dipahami menjadi informasi yang dapat dipahami. Berdasarkan kunci yang dipakai, algoritma kriptografi dibagi

menjadi dua yaitu algoritma simetris dan asimetris. Algoritma simetris memakai kunci yang sama dalam proses enkripsi dan proses dekripsi, sedangkan algoritma asimetris memakai kunci yang berbeda.

Kriptografi dibagi menjadi dua jenis yaitu kriptografi klasik dan kriptografi modern. Di dalam kriptografi klasik ada beberapa teknik yaitu teknik substitusi, teknik transposisi, teknik *blocking*, teknik ekspansi, dan teknik perambatan. Teknik kriptografi klasik merupakan teknik penyandian sederhana dan tingkat keamanannya relatif rendah sehingga dapat dibobol oleh pihak yang tidak bertanggung jawab. Oleh karena itu untuk meminimalisir hal tersebut, keamanan penyandiannya perlu ditingkatkan lagi.

Super enkripsi merupakan kombinasi dari teknik penyandian substitusi dan teknik penyandian transposisi untuk meningkatkan keamanan pesan yang akan dikirim. Dalam penelitian ini, Vigenere *cipher* yang merupakan teknik penyandian substitusi akan dikombinasikan dengan *route cipher* yang merupakan teknik penyandian transposisi. Vigenere *cipher* dan *route cipher* termasuk ke dalam kriptografi klasik yang menggunakan algoritma simetris. Kedua teknik ini dipilih karena relatif mudah dilakukan di komputer, gabungan dari kedua teknik ini akan melipat gandakan tingkat keamanan pesan.

Salah satu alternatif untuk keamanan pesan digital adalah dengan mengimplementasikan algoritma super enkripsi Vigenere *cipher* dan *route cipher*. Karena data atau pesan bersifat digital, maka implementasi algoritma tidak dilakukan secara manual. Pada penelitian ini, algoritma tersebut akan diimplementasikan menggunakan bahasa pemograman PHP. Berdasarkan uraian diatas maka peneliti akan menyusun penelitian yang berjudul "*Implementasi Algoritma Super Enkripsi Vigenere Cipher dan Route Cipher*

pada Penyandian Pesan Teks".

1.2 Rumusan Masalah

Permasalahan pada penelitian ini adalah bagaimana mengimplementasikan algoritma super enkripsi Vigenere *cipher* dan *route cipher* pada enkripsi dan dekripsi penyandian pesan teks, agar dapat mengamankan informasi rahasia pada pesan teks.

1.3 Batasan Masalah

Masalah penelitian ini hanya membahas tentang proses enkripsi dan dekripsi menggunakan Vigenere *cipher* yang kemudian dikombinasikan dengan *route cipher* menggunakan algoritma enkripsi yang dibaca spiral searah jarum jam dan kunci berupa bilangan asli yang kurang dari 6. Teknik penyandian dalam penelitian ini menggunakan kode ASCII untuk menyandikan pesan teks.

1.4 Tujuan Penelitian

Penelitian ini bertujuan untuk mengimplementasikan algoritma super enkripsi Vigenere *cipher* dan *route cipher* pada penyandian pesan teks.

1.5 Sistematika Penulisan

Secara keseluruhan sistematika penulisan dalam penelitian ini terdiri dari empat bab, yaitu Bab I, bagian pendahuluan berisikan latar belakang, rumusan masalah, tujuan penelitian, pembatasan masalah, dan

sistematika penulisan. Bab II, mengenai tinjauan pustaka berisikan teori-teori yang berhubungan dengan masalah yang dibahas. Bab III, bagian pembahasan berisikan tentang proses implementasi algoritma pada pesan atau data. Bab IV, bagian penutup berisi kesimpulan dan saran.