

BAB I

PENDAHULUAN

1.1. Latar Belakang Masalah

Kemajuan teknologi saat ini mengalami perkembangan yang cukup baik sehingga mempermudah keterbukaan terhadap akses data dan informasi. Hal ini juga berpengaruh pada kebutuhan pertukaran informasi yang sangat besar. Pertukaran informasi banyak dilakukan melalui media digital yaitu yang mencakup pada dunia hiburan, berita hingga pendidikan. Namun pertukaran informasi melalui media digital tidak menjamin akan keamanan informasi tersebut karena informasi dapat disalahgunakan oleh orang lain, pengguna membutuhkan suatu jaminan yang dapat meyakinkan mereka bahwa informasi yang diperoleh merupakan informasi yang benar dan aman. Oleh karena itu diperlukan suatu penyandian pesan dan informasi untuk meningkatkan keamanan suatu informasi.

Salah satu bidang ilmu untuk meningkatkan keamanan suatu informasi adalah kriptografi. Kriptografi merupakan studi yang bertujuan untuk mengamankan dan merahasiakan suatu informasi dengan melakukan proses enkripsi dan dekripsi. Enkripsi pesan dilakukan untuk menyembunyikan atau mengubah pesan yang bersifat rahasia menjadi sesuatu yang tidak bermakna dengan maksud agar tidak dapat terbaca oleh orang lain. Sedangkan dekripsi merupakan proses pengembalian data dalam bentuk sandi kedalam bentuk semula yang dapat dipahami dan memiliki sebuah makna. Dalam algoritma kriptografi juga terdapat istilah cipertext dan plainteks. Cipertext merupakan informasi atau pesan yang telah disandikan kedalam bentuk tertentu agar pesan tidak dapat dimengerti oleh pihak yang tidak berkepentingan. Sedangkan plainteks merupakan informasi atau pesan yang dapat dipahami maknanya[1]. Pada penelitian ini menggunakan huruf korea (hangul) sebagai cipertext untuk mengenkripsi sebuah pesan alfabet. Dalam bahasa korea, kalimat atau kata dibentuk oleh karakter-karakter sehingga algoritma kriptografi akan mengenkripsi pesan berdasarkan karakter per karakter.

Huruf Korea (Hangul) diperkenalkan oleh King Sejong sebagai huruf yang mudah dipelajari agar orang awam dapat membaca dan menulis. Pada huruf Korea (Hangul) terdapat 21 huruf yang mewakili bunyi vokal dan 19 huruf mewakili bunyi konsonan. Huruf-huruf tersebut digabungkan untuk membentuk sebuah karakter. Hangul tersusun atas jamo (*building blocks*) yang umumnya terdiri dari tiga elemen, yaitu awalan (*initial*), penengah (*medial*) dan penutup (*final*). Elemen final tidak selalu harus ada. Elemen inisial harus ada dan harus berupa bunyi konsonan. Elemen medial harus ada dan harus berupa bunyi vokal[2]. Untuk menyusun cipertexts dalam huruf korea (hangul) akan diimplementasikan algoritma *finite state automata* untuk penentuan pola suku kata.

Finite State Automata (FSA) merupakan *tools* yang sangat berguna untuk mengenal dan menangkap pola dalam data. *Finite State Automata (FSA)* merupakan model matematika yang dapat menerima input dan mengeluarkan output yang memiliki state berhingga dan dapat berpindah dari satu state ke state lainnya berdasarkan input dan fungsi transisi. *Finite State Automata (FSA)* merupakan jenis otomata yang tidak memiliki penyimpanan, sehingga kemampuan mengingatnya terbatas. [3].

Sistem proses rancangan pada enkripsi pesan ini yaitu string alfabet atau pesan asli yang diperoleh akan dikonversi kedalam bentuk huruf korea dengan menentukan sebuah kunci sebagai kata penentu enkripsi. Pembangkit kunci merupakan sebuah kalimat yang panjang. Pola suku kata pada pesan atau kata alfabet akan ditransisi menggunakan implementasi algoritma *finite automata*. Algoritma *finite automata* digunakan untuk menentukan pola suku kata diterima atau ditolak oleh sistem sehingga pesan dapat dienkripsi ke dalam huruf Korea (Hangul). Penyusunan cipertexts huruf Korea akan ditulis sesuai dengan kaidah penulisan dalam huruf Korea.

1.2. Rumusan Masalah

Berdasarkan uraian latar belakang diatas, maka dapat dirumuskan masalah sebagai berikut :

1. Bagaimana mengenkripsi pesan alfabet menjadi bentuk huruf Korea

(hangul) dengan menggunakan implementasi finite automata sebagai penentuan pola suku kata?

2. Bagaimana mengimplementasikan finite automata untuk menyusun chiperteks dalam huruf Korea (hangul) sesuai dengan kaidah penulisan huruf Korea ?

1.3. Tujuan Penelitian

Tujuan penelitian adalah sebagai berikut :

1. Mengubah pesan alfabet kedalam bentuk huruf Korea (hangul) untuk menjaga keamanan dan kerahasiaan informasi.
2. Mengimplementasikan finite automata untuk menentukan pola suku kata sesuai dengan kaidah penulisan huruf Korea (hangul).
3. Melakukan pengujian hasil enkripsi pesan alfabet kedalam huruf Korea (hangul) dengan implementasi algoritma finite automata.

1.4. Batasan Masalah

Dalam pembuatan dan perancangan sistem terdapat batasan masalah sebagai berikut :

1. Mengubah pesan alfabet menjadi huruf Korea (hangul) menggunakan kaidah penulisan huruf Korea meskipun teks enkripsi tersebut tidak memiliki makna dalam bahasa Korea.
2. Pesan alfabet yang di enkripsi tidak termasuk angka, spasi, tanda baca dan karakter huruf lainnya, diasumsikan bahwa pesan yang diinputkan hanya mengandung huruf alfabet.
3. Terdapat beberapa huruf Hangul yang tidak digunakan dalam proses enkripsi pesan.

1.5. Manfaat Penelitian

Manfaat dari penelitian ini adalah sebagai berikut :

1. Bagi penulis, dapat menerapkan dan mengembangkan ilmu kriptografi pada enkripsi dan dekripsi pesan serta dapat menambah pengetahuan mengenai huruf Korea beserta cara penulisannya.

2. Bagi khalayak umum, penelitian ini dapat dijadikan sebagai media alternatif untuk mengamankan pesan menjadi bentuk lain sehingga pesan yang dikirimkan terjaga keamanan dan kerahasiaannya.