BAB I

PENDAHULUAN

1.1. Latar Belakang

Banyaknya aksi penyadapan yang perlu kita sikapi dengan serius karena aksi penyadapan tersebut telah melanggar hak asasi manusia dalam berkomunikasi dengan aman, dalam hal ini adalah komunikasi melalui surat elektronik dengan akses internet atau dikenal dengan email. Data atau isi pesan yang ada pada email tersebut harus dijaga kerahasiaan data pesan salah satunya dengan menggunakan ilmu *kriptografi*. Ilmu *kriptografi* adalah salah satu teknik untuk mengamankan data atau pesan. Pengamanan data dapat dilakukan dengan berbagai algoritma, salah satunya yang sudah lama perkembangannya dengan menggunakan Algoritma *Caesar* dan *Vigenere.*

Algoritma *Caesar* dan *Vigenere* merupakan bagian dari awal perkembangan ilmu *kriptografi* atau bagian dari *kriptograf*i klasik. Oleh karena itu oleh peneliti yang terdahulu dalam papernya yang di tulis oleh O.E Omolara dan A.I Oludare menyebutkan mengkombinasi kedua metode enkripsi ini yang mana merupakan metode enkripsi yang dilakukan pergeseran huruf dengan angka dilanjutkan dengat teks. Penggabungan dua kunci ini merupakan salah satu metode yang komplek dalam pengoperasiannya. Algoritma ini memanfaatkan pergeseran huruf yang ada pada data atau pesan yang akan diamankan menggunakan sebuah kunci berupa jumlah pengeseran dan kata atau susunan kata untuk proses pengacakan data atau pesan. Proses yang dilakukan adalan proses enkripsi dan deskripsi.

Pada studi kasus ini akan membahas mengenai penerapan kombinasi Algoritma *Caesar* dan *Vigenere* untuk pengamanan data pesan pada surat elektronik, agar data atau isi pesan dapat dilindungi dari tindakan penyadapan yang sedang marak dilakukan.

Dari uraian singkat di atas maka penulis akan membuat sebuah aplikasi yang digunakan untuk "Penerapan Kombinasi Algoritma *Caesar* dan *Vigenere* Untuk Pengamanan Data Pesan pada Surat Elektronik". Untuk implementasi pembuatan aplikasinya menggunakan bahasa pemprograman PHP berbasis web dan hasil akhir dari aplikasi adalah dapat mengamankan data pesan yang akan dikirim.

1.2. Rumusan Permasalahan

Berdasarkan latar belakang tersebut maka dapat dirumuskan masalah, yaitu Bagaimana menerapkan kombinasi Algoritma *Caesar* dan *Vigenere* untuk melindungi isi pesan pada pesan elektronik yang akan dikirim.

1.3. Batasan Masalah

Berdasarkan rumusan masalah di atas maka permasalahan yang perlu dibahas sebagai berikut :

1. Sistem hanya berupa simulasi pengiriman pesan elektronik
2. Metode yang digunakan adalah Algoritma *Caesar* dan *Vigenere*
3. Bahasa pemrograman menggunakan PHP

1.4. Tujuan

Adapun tujuan dari tugas akhir ini adalah mengimplementasikan penerepan kombinasi dari algoritma *Caesar* dah *Vigenere* untuk pengamanan data pesan pada surat elektronik.

1.5. Manfaat

Adapun Manfaat dari penerapan kombinasi algoritma *Caesar* dan *Vigenere* untuk pengamanan data pesan pada surat elektronik ini adalah:

1. Manfaat bagi pembaca: membantu pembaca untuk mendapatkan rasa aman dalam melakukan komunikasi sehingga tidak khawatir isi pesan pribadinya dilihat oleh orang lain.
2. Manfaat bagi pembaca: menambah pengetahuan pengetahuan teknik pengamanan data atau *kriptogafi* dalam mengamankan data pesan pada surat elektronik.
3. Manfaat bagi peneliti lain: sebagai referensi dalam penelitian yang memiliki topik yang sama atau yang menggunakan metode yang sama.
4. Manfaat bagi penulis: menambah pengetahuan dalam teknik *kriptografi* klasik yang banyak digunakan untuk pengaman data-data elektronik dan memperdalam berbagai macam teknik teknik lanjutan dalam *kriptografi*.

1.6. Sistematika Penulisan

Sistematika penulisan Tugas Akhir ini disusun kedalam lima bab. Bab - bab tersebut terdapat daftar pustaka serta lampiran. Adapun dari kelima bab tersebut adalah :

BAB I: PENDAHULUAN

Didalam bab ini membahas tentang latar belakang, rumusan masalah, batasan masalah, tujuan, manfaat dari aplikasi dan sistematika penulisan tugas akhir.

BAB II: TINJAUAN PUSTAKA

Pada bab ini membahas tentang teori teori yang mendukung serta metode yang digunakan dalam melakukan enkripsi dan deskripsi.

BAB III: METODOLOGI PENELITIAN

Pada bab ini membahas tentang metodologi penelitian sistem dalam pembuatan aplikasi, seperti diagram sistem, daftar tabel, flowchart, dan sketsa rancangan aplikasi.

BAB IV: HASIL DAN PEMBAHASAN

Pada bab ini akan dijelaskan mengenai kebutuhan perangkat keras maupun perangkat lunak serta output dari aplikasi ini, termasuk penjelasan tentang penggunaan aplikasi. Serta dilakukannya ujicoba aplikasi yang telah dibuat. Proses ujicoba akan menguji output yang dihasilkan, apakah telah sesuai dengan tujuan yang telah ditentukan.

BAB V: KESIMPULAN DAN SARAN

Pada bab ini berisi kesimpulan terhadap aplikasi yang telah dibuat serta saran bagi pengembangan aplikasi selanjutnya.

DAFTAR PUSTAKA

Pada bagian ini akan dipaparkan tentang sumber-sumber literatur yang digunakan dalam pembutan laporan ini.