BAB I

PENDAHULUAN

1.1 Latar Belakang Masalah

Kriptografi klasik merupakan kriptografi yang sudah ada sejak dulu sebelum komputer ada. Kriptografi ini dilakukan dengan algoritma berbasis karakter. Algoritma yang digunakan termasuk ke dalam sistem kriptografi simetri dan digunakan jauh sebelum sistem kriptografi kunci publik ditemukan. Terdapat sejumlah algoritma yang tercatat dalam sejarah kriptografi, sehingga dinamakan algoritma kriptografi klasik. Salah satu contoh kriptografi klasik yaitu metode *Caesar Cipher* yang digunakan oleh Kaisar Julius Caesar untuk mengirimkan pesan sandi kepada para tentaranya agar tidak diketahui oleh musuh.

Namun dengan seiringnya perkembangan teknologi yang semakin canggih pada masa sekarang ini, algoritma klasik tersebut sudah tidak di gunkana lagi karena algoritma tersebut mudah untuk dipecahkan. Tetapi berkembangnya algoritma – algoritma modern yang ada pada saat ini merupakan pengembangan dari algoritma klasik, dan algoritma klasik yang ada merupakan dasar dari pengembangan algoritma kriptografi modern. Oleh karena itu, penelitian tentang kriptografi akan selalu berkembang untuk memperoleh algoritma kriptografi yang semakin kuat, sehingga usaha - usaha untuk memecahkan kode kriptografi secara tidak sah menjadi lebih sulit.

1.2 Maksud

Maksud dari penulisan karya ilmiah ini adalah untuk memberikan pemahaman konsep dasar kriptografi metode klasik, dengan membandingkan cara kerja dari tiga metode kriptografi klasik yaitu metode *Caesar Cipher,*

Columnar Transposition dan *Vigenere Cipher*, serta mengimplementasikannya ke bahasa pemrograman.

1.3 **Tujuan**

Tujuan penyusunan Karya Ilmiah ini adalah:

a. Menambah khasanah atau wawasan ilmu pengetahuan khususnya dalam bidang *scurity* (keamanan) dan pemrograman.
b. Sebagai kontribusi kepada dunia ilmu pengetahuan dan teknologi khususnya ilmu komputer.
c. Masyarakat dapat memahami konsep kriptografi *Cipher Classic* khususnya metode *Caesar Cipher, Columnar Transpotition* dan *Vigenere Cipher.*

1.4 **Batasan Masalah**

Dalam implementasi Kriptografi *Cipher Classic* ini, penulis hanya bertumpu pada tiga metode yaitu metode *Ceasar Cipher, Columnar Transposition* dan *Vigenere Cipher*. Dari ketiga metode tersebut, penulis hanya membandingkan cara kerjanya antara cara manual dan di implementasikan dengan program bantu tanpa melalui adanya proses penyimpanan hasil enkripsi, serta menganalisis hasil enkripsi dari ketiga metode tersebut.

1.5 Metode Pengumpulan Data

Untuk membantu kelancaran dan mempermudah penyusunan Karya Ilmiah ini diperlukan data - data yang akurat. Untuk memperoleh data - data dan merancang sistem ini, metode penelitian yang digunakan adalah dengan Studi Pustaka yaitu suatu metode pengumpulan data dengan cara mempelajari

referensi dari buku-buku dan karya tulis yang sesuai dengan permasalahan. Dari studi pustaka ini diperoleh langkah - langkah pembuatan karya tulis secara baik dan benar.

1.6 Sistematika Penulisan

Agar hasil dari penulisan karya ilmiah ini dapat dimengerti dan dipahami oleh pembaca, maka dalam penyusunan laporan karya ilmiah ini dibagi menjadi lima bagian, yaitu Bab I merupakan pendahuluan, dalam bagian ini akan diuraikan mengenai latar belakang masalah, maksud dan tujuan, batasan masalah serta sistematika penulisan.

Bab II merupakan landasan teori, yang akan mencakup teori tentang kriptografi dan metode – metode yang digunakan untuk dijadikan acuan dalam pembahasan penyusunan laporan karya ilmiah ini, serta tentang bahasa pemrograman yang digunakan untuk membuat program bantu oleh penulis.

Bab III merupakan analisis dan perancangan yang menjelaskan tentang diagram alir enkripsi dan dekripsi dari tiap metode, penjelasan sistem, dan perencanaan form serta perancangan input output.

Bab IV merupakan implementasi dan pembahasan, pada bab IV ini berisi pembahasan dari hasil awal berupa metode perancangan dan hasil perancangan untuk kemudian diimplementasikan dalam program dengan menggunakan bahasa pemrograman Visual Basic 6.0.

Bab V Penutup merupakan bab terakhir yang menguraikan kesimpulan dan saran - saran dari hasil karya ilmiah yang telah dibuat, yang dapat membantu untuk proses pengembangan di masa mendatang.