BAB I

PENDAHULUAN

1.1 Latar Belakang

Kriptografi adalah metode yang digunakan untuk melindungi kerahasiaan data. Kriptografi memiliki ciri ciri enkripsi bernilai sama dengan dekripsi. Enkripsi adalah proses merubah data menjadi kode-kode rahasia, sedangkan dekripsi adalah kode-kode rahasia yang diproses kembali menjadi data atau informasi. Berikut merupakan macam-macam kriptografi yaitu caesar cipher, vigenere cipher, playfair cipher, DES, 2DES, 3DES, AES, RC2, RC3, RC4, RC5, RC6, Blowfish, GHOST, LOKI, IDEA, dan lain-lain (Hidayat, 2009). Caesar cipher adalah salah satu jenis kriptografi yang menggunakan metode substitusi monoalphabet, dimana setiap karakter enkripsi menggantikan satu karakter asli. Algoritma ini merupakan salah satu jenis algoritma klasik yang memiliki pola simetris.

American Standart Code for Information Interchange (ASCII) merupakan tabel kriptografi yang digunakan untuk memaksimalkan pengamanan informasi berupa pesan. ASCII adalah sebuah kode standar yang digunakan dalam pertukaran informasi pada Komputer. Jumlah kode ASCII adalah 255 kode. Kode ASCII 0 – 127 merupakan kode ASCII untuk manipulasi teks, sedangkan kode ASCII 128 – 255 merupakan kode ASCII untuk manipulasi grafik. ASCII memiliki karakter kontrol yang dibedakan menjadi 5 kelompok sesuai dengan penggunaan berturut-turut yaitu meliputi *Logical Communication, Device Control, Information Separator, Code Extention, dan Physical Communication.* Code ASCII ini banyak dijumpai pada papan ketik komputer atau instrumen-instrumen digital.

Salah satu bagian unicode pada ASCII adalah karakter noncetak kontrol ASCII atau sering disebut "*ASCII Character Control*". Karakter ini jarang sekali dipergunakan secara umum, namun juga sering digunakan untuk

kontrol pada komputer. Sehingga dalam pengimplementasiannya karakter ini merupakan karakter *Non-Printable*. Dan sangat mendukung dalam mengenkripsi data dan Informasi.

Pada aplikatifnya, Caesar cipher mudah dipecahkan dengan metode *exhaustive key* search karena jumlah kuncinya sangat sedikit (hanya ada 26 kunci) (Munir, 2004). Namun dengan adanya kode ASCII *Non-Printable* yang diterapkan, tingkat kesulitan dalam proses decodenya akan lebih rumit. Karena kita mencoba untuk menerapkan metode klasik dengan sistem modern.

1.2 Rumusan Masalah

Berdasarkan latar belakang tersebut, maka rumusan masalah yang dapat dikaji adalah Mengkombinasikan karakter kontrol ASCII dengan Algoritma Kriptografi Caesar Cipher sehingga terbentuk suatu model kriptografi klasik yang diperbarui.

1.3 Tujuan

Memanfaatkan Karakter Kontrol ASCII untuk memodifikasi Kriptografi Substitusi khususnya algoritma Caesar Cipher

1.4 Manfaat

Dapat dimanfaatkan dalam penyimpanan data data rahasia atau penting, sehingga dapat meningkatkan keamanan data.

1.5 Batasan Masalah

1. Metode yang digunakan menggunakan Metode Kriptografi Substitusi Algoritma Caesar Cipher
2. Menggunakan dasar bilangan ASCII
3. Pengujian difokuskan pada file berbentuk Alfanumerik