BAB I

PENDAHULUAN

1.1 Latar Belakang

Kriptografi merupakan bidang pengetahuan yang menggunakan persamaan matematis untuk melakukan proses enkripsi maupun deskripsi. Teknik ini digunakan untuk mengkonversi data kedalam bentuk kode-kode tertentu sehingga menjadi susunan huruf yang tidak dapat dibaca. Dalam kriptografi sendiri terdiri dari beberapa algoritma atau metode-metode diantaranya *Affine Cipher, Base 64* dan *Vigenere Cipher.* Dari ketiga algoritma tersebut mungkin didapati *efisiensi* yang berbeda-beda, dimana *efisien* tidaknya algoritma kriptografi mengarah pada kecepatan dalam mengenkripsi atau mendekripsi data dan besaran ukuran *file* yang dihasilkan.

Dan masing-masing algoritma mempunyai kelebihan serta kekurangan, pada algoritma kriptografi *affine cipher* ini terdapat kelebihan yaitu terletak pada pertukaran huruf-huruf yang akan disandikan dengan huruf-huruf itu sendiri, sehingga keteraturan huruf itu menjadi acak. Dan kekuatan *cipher* itu terletak pada kunci yaitu nilai integer yang menunjukan pergeseran karakter-karakter. Sedangkan kelemahan algoritma ini adalah mudah diserang dengan hanya melihat ciphertextnya

karena dengan melihat frekuensi chiperteks terbanyak disesuaikan dengan banyaknya frekuensi pada plainteks pada umumnya. Karena kunci dalam *affine cipher* hanya 25 kemungkinan kunci untuk alfabet dan 128 kemungkinan kunci untuk *ASCII*.

Algoritma *base-64* juga mempunyai kelebihan yaitu pada prosesnya sudah menggunakan operasi dalam *mode bit* sehingga akan menjadikan karakter-karakter acak yang tidak dapat dimengerti karena sudah merepresentasikan data biner kedalam format *ASCII*.

Sedangkan algoritma *vigenere cipher* sendiri cukup rumit untuk dipecahkan, meskipun begitu *vigenere cipher* tetap memiliki kelemahan salah satunya dapat diketahui panjang kuncinya dengan menggunakan metode kasiski yaitu merupakan metode untuk mencari panjang kunci sehingga menyebabkan *vigenere cipher* mudah dipecahkan. Namun semakin pajang kunci yang diberikan apalagi sepanjang plainteks yang ada, maka kemungkinan *vigenere cipher* dipecahkan semakin sulit.

1.2 Rumusan Masalah

Dari permasalahan diatas , maka dirumuskan untuk dibuat sebuah perangkat lunak aplikasi untuk membandingkan algoritma kriptografi *affine cipher, base-64,* dan *vigenere cipher* yang digunakan dalam menangani proses *enkripsi-dekripsi* serta menampilkan beberapa informasi yang merepresentasikan kinerja masing-masing algoritma berdasarkan hasil pengujian terhadap setiap proses yang ditangani. Informasi tersebut akan dijadikan sebagai acuan analisis perbandingan antara ketiga algoritma kriptografi tersebut.

1.3 Ruang Lingkup Masalah

Mengingat luasnya permasalahan yang timbul maka diperlukan batasan untuk menghindari meluasnya masalah dalam pembahasan, yaitu:

1. Aplikasi yang akan dibangun menangani proses enkripsi-dekripsi algoritma kriptografi *affine cipher, base-64* dan *vigenere cipher* terbatas pada file teks saja.
2. Perhitungan waktu pemrosesan ditangani kode program dengan mengambil waktu sistem tepat sebelum proses

dimulai dan tepat setelah proses selesai,kemudian menghitung selisih waktunya.

3. Basis bilangan yang digunakan adalah *ASCII 128*
4. Analisis meliputi :
   - Analisis waktu yang dibutuhkan dalam proses enkripsi dan dekripsi.
   - Analisis perubahan ukuran file terhadap proses enkripsi dan dekripsi.
   - Analisis waktu proses terhadap pengaruh aplikasi yang sedang berjalan.

1.4 Tujuan Penelitian

Tujuan dari karya tulis ini adalah membangun suatu aplikasi untuk menganalisis *performansi* data dari algoritma kriptografi *affine cipher, base-64,* dan *vigenere cipher.*