BAB I
PENDAHULUAN

1. 1. Latar Belakang Masalah

Perkembangan teknologi informasi memberikan kemudahan manusia berkomunikasi dengan dunia luar untuk saling bertukar pesan ataupun data antara satu dengan yang lainnya. Kerahasiaan pesan ataupun data sangat penting bagi suatu perusahaan atau organisasi. Kerahasiaan pesan ataupun data seseorang dikategorikan sebagai hal penting dalam pengiriman pesan ataupun data supaya hanya dapat diberikan orang tertentu untuk mengakses informasi pesan atau data yang dituju.

Umumnya pesan atau data ini dikategorikan menjadi 2 jenis yakni pesan ataupun data yang bersifat rahasia dan pesan ataupun data yang bersifat tidak rahasia. Pesan ataupun data yang bersifat rahasia ini perlu teknik khusus supaya tetap terjaga kerahasiaannya. Sedangkan pesan ataupun data yang bersifat tidak rahasia tidak perlu teknik khusus dikarenakan orang lain dapat dengan mudah mengetahui isi pesan ataupun data.

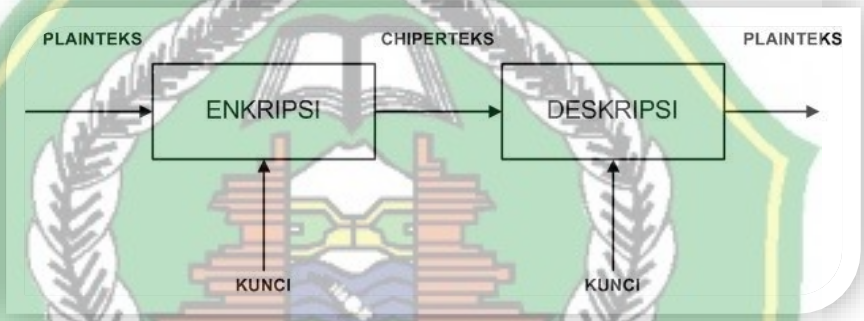
Pada era saat ini, banyak sekali ancaman pencurian data oleh pihak lain yang tidak berkepentingan. Data tersebut kebanyakan data pribadi sehingga sangat meresahkan apabila disalahgunakan oleh oknum yang tidak bertanggungjawab. Pencurian data pribadi melalui jaringan internet marak dialami oleh masyarakat umum karena akses internet yang tanpa batas. Terkait permasalahan tersebut untuk menjaga keamanan pesan ataupun data yang bersifat rahasia memerlukan teknik khusus yang digunakan untuk menyandikan data-data yang berupa file serta untuk membukanya memerlukan kunci rahasia yang sulit untuk dideteksi oleh pihak manapun yang tidak bersangkutan.

Kerahasiaan pesan ataupun data dapat diubah ke dalam bentuk penyandian dengan memanfaatkan ilmu dalam matematika yaitu kriptografi. Kriptografi berasal dari Bahasa Yunani. Dalam segi Bahasa, Kriptografi berasal

dari dua kata yaitu *kripto* dan *graphia. Kripto* diartikan *secret* (rahasia) dan *graphia* diartikan *writing* (tulisan). Menurut Terminologi, Kriptografi adalah ilmu dan seni untuk menjaga keamanan pesan ketika pesan dikirim dari suatu tempat ke tempat yang lain (Ariyus, 2006).

(Munir R. , 2006) menyebutkan bahwa pesan asli yang dapat dibaca disebut plaintext dan teks yang sudah disandikan disebut ciphertext. Proses penyandian pesan ataupun data terdiri dari 2 proses yakni proses untuk mengubah dari plaintext menjadi ciphertext disebut enkripsi dan proses mengubah dari ciphertext menjadi plaintext disebut deskripsi.

Gambaran proses penyandian enkripsi – deskripsi :



Gambar 1.1 Proses Penyandian

(Sumber : Munir, 2006)

(Ariyus, Pengantar Ilmu Kriptografi : Teori, Anaisis dan Implementasi, 2008) menyebutkan bahwa berpatok pada kunci yang dipakai, algoritma kriptografi dikategorikan menjadi tiga yakni algoritma asimetri, algoritma simetri serta fungsi hash. Kriptografi pula dikategorikan menjadi dua jenis yaitu kriptografi klasik dan kriptografi modern. Beberapa teknik dalam kriptografi klasik diantaranya teknik substitusi, teknik *blocking*, teknik permutasi, teknik perampatan serta teknik ekspansi. Beberapa macam teknik substitusi diantaranya Caesar Chiper, Shift Chiper, Vigenere Chiper, Hill Chiper serta Playfair Chiper.

Caesar Chiper dan Hill Chiper termasuk dalam kategori kriprografi klasik yang menggunakan teknik substitusi. Peneliti memilih Caesar Chiper dan Hill Chiper karena akan menghasilkan keamanan yang lebih kuat serta mampu

mengetahui konsep-konsep kriptografi yang memanfaatkan ilmu matematika yakni matriks dan aritmatika modular. Penelitian ini dilakukan sebagai bahan pembelajaran bagi pihak yang berkaitan dengan penyandian maupun kriptografi dikarenakan masih sedikit yang membahas permasalahan ini. Peneliti berharap penelitian ini dapat memberikan manfaat untuk dijadikan acuan mengenai penelitian kriptografi.

Berdasarkan latar belakang tersebut, penelitian ini akan melakukan penyandian dan penguraian sandi menggunakan ilmu matematika dengan judul "Analisis Hill Cipher dan Caesar Cipher Menggunakan Matriks dan Aritmatika Modular"

1. 2. Identifikasi Masalah

Berdasarkan latar belakang masalah diatas, permasalahan yang berhasil penulis identifikasi adalah:

1. Bagaimana penyandian data Hill Cipher menggunakan matriks
2. Bagaimana penyandian data Caesar Cipher menggunakan aritmatika modular
3. Bagaimana penyandian data gabungan Hill Cipher dan Caesar Cipher menggunakan matriks dan aritmatika modular

1. 3. Batasan Masalah

Berdasarkan identifikasi masalah yang sudah penulis jelaskan diatas, penelitian ini dibatasi:.

1. Pada Hill Cipher hanya membahas perbedaan hasil yang menggunakan kunci matriks $2 \times 2, 3 \times 3$, dan 4×4.
2. Pada Caesar Cipher berpatokan kepada pergeseran huruf yang menggunakan metode blok, karakter dan zig-zag.

1. 4. Rumusan Masalah

Berdasarkan identifikasi masalah dan batasan penelitian diatas, rumusan masalah pada penelitian ini adalah:

1. Bagaimana penyandian data Hill Cipher menggunakan matriks?
2. Bagaimana penyandian data Caesar Cipher menggunakan aritmatika modular?
3. Bagaimana penyandian data gabungan Hill Cipher dan Caesar Cipher menggunakan matriks dan aritmatika modular?

1. 5. Tujuan Penelitian

Berdasarkan rumusan masalah diatas, tujuan penelitian ini adalah:

1. Untuk mengetahui penyandian data Hill Cipher menggunakan matriks.
2. Untuk mengetahui penyandian data Caesar Cipher menggunakan aritmatika modular.
3. Untuk mengetahui penyandian data gabungan Hill Cipher dan Caesar Cipher menggunakan matriks dan aritmatika modular

1. 6. Manfaat Hasil Penelitian

Manfaat yang dapat diperoleh dari penelitian ini adalahh:

1. Manfaat Teoritis

   Secara teoritis, penelitian ini diharapkan dapat memberikan gambaran tentang penyandian Hill Chiper dan Caesar Cipher dengan aplikasi matriks dan aritmatika modular

2. Manfaat Praktis

   a. Penulis

      Sebagai pembelajaran untuk memahami penyandian Hill Chiper dan Caesar Cipher dengan aplikasi matriks dan aritmatika modular*)*, sehingga dapat menambah wawasan ilmu pengetahuan pada bidang kriptografi.

b. Mahasiswa

Sebagai bahan rujukan mengenai penyandian Hill Chiper dan Caesar Cipher dengan aplikasi matriks dan aritmatika modular.

c. Lembaga

Sebagai inventaris teori dalam pengembangan penyandian Hill Chiper dan Caesar Cipher dengan aplikasi matriks dan aritmatika modular.