BAB I
PENDAHULUAN

1.1 Latar Belakang

Kemajuan teknologi memudahkan orang untuk mengakses informasi. Hal ini dimanfaatkan oleh orang-orang tertentu untuk menyalahgunakannya. Pelaku kejahatan komputer (*cyber crime*) atau sering pula disebut *hacker, cracker* atau dengan sebutan lainnya biasa melakukan kegiatannya dengan mengubah makna suatu informasi, sehingga informasi yang diterima oleh penerima berbeda dengan yang sebenarnya disampaikan oleh pengirim. Hal ini sangat mengganggu privasi seseorang. Oleh karena itu, perlu adanya sistem atau aplikasi yang aman untuk digunakan pengguna teknologi dalam hal mengamankan informasi yang dimilikinya.

Banyak cara untuk mempersulit pelaku kejahatan komputer, salah satunya dengan mengubah pesan yang dikirimkan menjadi sebuah pesan yang tidak terbaca, sehingga hanya pengirim dan penerima pesan saja yang dapat membaca pesan tersebut. Salah satu cabang ilmu yang mempelajari teknik tersebut adalah kriptografi. Kriptografi adalah ilmu dan seni untuk menjaga keamanan pesan ketika pesan dikirim dari suatu tempat ke tempat lain (Ariyus D. 2013). Kriptografi erat kaitannya dengan ilmu matematika diantaranya teori bilangan, aljabar abstrak, teori peluang dan logika matematika. Teknik kriptografi sudah digunakan sejak jaman dahulu, dari era perang kekaisaran romawi, sampai perang dunia kedua oleh tentara Jerman yang menggunakan mesin "Enigma". Pada masa kini, kriptografi banyak diaplikasikan dalam kehidupan seperti penggunaan mesin ATM, *fingerprint scanner*, alat-alat komunikasi, serta transaksi yang menggunakan Internet.

Sebelum era modern seperti saat ini, kriptografi dilakukan dengan menuliskannya pada selembar kertas. Teknik tersebut dinamakan teknik kriptografi klasik. Salah satu contoh dari kriptografi klasik adalah algoritma *Hill Cipher*. *Hill Cipher* merupakan teknik kriptografi yang menggunakan penerapan

aritmatika modulo dan aljabar matriks. Teknik ini menggunakan matriks persegi sebagai kunci untuk melakukan proses enkripsi dan dekripsi. Teknik ini dapat bertahan dari serangan analisis frekuensi karena setiap karakter yang dienkripsi memiliki keterkaitan satu sama lain. Namun teknik ini dapat dipecahkan dengan teknik *known-plaintext*, dimana kriptanalis yang memiliki potongan *plaintext* dapat melakukan teknik perkalian matriks ataupun persamaan linear untuk mendapatkan kuncinya. Maka dari itu diperlukan suatu modifikasi pada *Hill Cipher* sehingga tidak mudah terserang oleh *known-plaintext attack*.

Salah satu cara memodifikasi *Hill Cipher* adalah dengan menambahkan algoritma dan ukuran kunci matriksnya, sehingga pesan yang disandikan akan lebih sulit dianalisis walaupun diketahui metodenya. Penambahan algoritma yang dimaksud adalah menambahkan variasi matriks dan mengulang proses pada algoritma *Hill Cipher* awal sebanyak yang diinginkan oleh pengguna. Sehingga, algoritma akan tampak seperti rantai. Maka dari itu, teknik tersebut dapat disebut sebagai metode *Chain Hill Cipher*. Selain menambah algoritma, banyaknya karakter yang dapat dienkripsi pun ditambah yang awalnya 26 karakter alfabet, ditambah 3 karakter yakni (spasi), (titik), dan (koma) sehingga banyaknya karakter menjadi 29 karakter. Hal ini dapat menambah peluang banyaknya kunci matriks yang dapat digunakan sehingga dapat mempersulit kriptanalis.

Proses enkripsi dan dekripsi dari *Chain Hill Cipher* menggunakan perhitungan matematika, terutama dalam menghitung perkalian matriks dan persamaan modulo. Maka dari itu, untuk mempermudah proses enkripsi dan dekripsi, perlu adanya program aplikasi yang dapat menghitung secara cepat. Salah satu program aplikasi yang memenuhi kriteria tersebut adalah program aplikasi yang dioperasikan menggunakan MATLAB. Dengan program aplikasi diharapkan pengguna dapat menggunakan algoritma *Chain Hill Cipher* dalam mengenkripsi dan mendekripsi pesan tanpa perhitungan yang rumit.

1.2 Rumusan Masalah

Masalah yang dikaji dalam skripsi ini adalah sebagai berikut.

1. Bagaimana menentukan algoritma kriptografi *Chain Hill Cipher*?

2. Bagaimana mengkonstruksi program aplikasi kriptografi *Chain Hill Cipher*?

1.3 Tujuan

Berdasarkan rumusan masalah di atas, tujuan dari penulisan skripsi ini adalah sebagai berikut.

1. Menentukan algoritma kriptografi *Chain Hill Cipher*.
2. Mengetahui konstruksi program aplikasi kriptografi *Chain Hill Cipher*.

1.4 Manfaat Penulisan

Melalui penulisan skripsi ini, diharapkan adanya manfaat terutama dalam bidang matematika terapan. Manfaat yang diharapkan yaitu :

1. Mempersulit kriptanalis dalam memecahkan algoritma kriptografi *Hill Cipher* dengan menggunakan teknik *known-plaintext attack*.
2. Mempermudah pengguna teknik *Chain Hill Cipher* dalam enkripsi dan dekripsi pesan dengan menggunakan program aplikasi.

1.5 Sistematika Penulisan

Sistematika penulisan skripsi ini mengacu pada pedoman penulisan karya tulis ilmiah Universitas Pendidikan Indonesia tahun 2011, dengan urutan sebagai berikut.

1. BAB I menjelaskan latar belakang, rumusan masalah, serta tujuan dan manfaat penulisan sebagaimana telah tertera diatas.
2. BAB II, diberikan konsep-konsep dasar yaitu aritmatika modulo, aljabar matriks, hingga konsep kriptografi klasik yang menunjang pengkajian dalam permasalahan skripsi ini.
3. BAB III akan dijelaskan mengenai tahap-tahap yang dilakukan penulis dalam menyelesaikan skripsi ini.
4. BAB IV berisi pembahasan, yaitu mengenai pembentukan algoritma, konstruksi program aplikasi, serta analisis mendalam tentang cara kerja program aplikasi kriptografi *Chain Hill Cipher*.

5. BAB V berisi kesimpulan dari hasil kajian dan rekomendasi untuk kajian selanjutnya yang berksinambungan dengan topik pada skripsi ini.