BAB I

PENDAHULUAN

1.1 Latar Belakang

Kriptografi adalah seni untuk mengamankan sebuah pesan yang bersifat rahasia dengan cara menyamarkannya agar tidak dapat dimengerti oleh siapapun kecuali pihak yang berhak mengetahuinya. Kriptografi dinyatakan dalam suatu kriptosistem yang terdiri atas *plaintext* atau pesan rahasia, *ciphertext* atau pesan yang tersamarkan, kunci kriptografi, dan algoritma untuk mengonversi *plaintext* ke dalam bentuk *ciphertext* dan sebaliknya. Proses mengonversi *plaintext* ke *ciphertext* disebut enkripsi dan proses sebaliknya disebut dekripsi. Suatu kriptosistem hanya dapat dilakukan oleh pihak yang berhak mengetahuinya. Namun, seiring perkembangan teknologi dan informasi dari masa ke masa seringkali pesan rahasia tersebut diretas oleh pihak yang tidak berhak mengetahui pesan tersebut atau dalam kriptografi disebut kriptanalis sehingga pengirim pesan harus meningkatkan keamanan pesan dengan mengembangkan kriptografi, diantaranya adalah memperbanyak jumlah kemungkinan kunci kriptografi atau menggabungkan dua buah kriptosistem.

Ada dua tipe algoritma kriptografi, yaitu algoritma simetri dan algortima asimetri. Algoritma simetri adalah algoritma yang menggunakan satu kunci privat yang hanya dimiliki oleh pemberi dan penerima pesan, contohnya adalah algoritma *hill cipher*. Sedangkan algoritma asimetri adalah algoritma yang menggunakan kunci privat dan kunci publik yang disebarkan secara umum, contohnya adalah *elliptic curve cryptography* (ECC).

Hill cipher sangat sulit untuk diretas apabila kriptanalis hanya mengetahui *ciphertext*nya atau dikenal dengan metode *ciphertext-only attack* karena sifat linearitasnya, yaitu setiap karakter memiliki keterikatan satu sama lain. Tetapi dengan metode *known plaintext attack*, seorang kriptanalis dapat

mengkriptanalisis *ciphertext* ketika memiliki sebagian *plaintext*nya, sehingga *hill cipher* menjadi tidak begitu aman akibatnya peningkatan keamanan harus dilakukan. Salah satu cara untuk meningkatkan keamanan pesan adalah menggabungkan *hill cipher* dengan *elliptic curve cryptography*. *Elliptic curve cryptography* dipilih karena hanya membutuhkan kunci dengan jumlah bit yang jauh lebih sedikit dibandingkan dengan kriptografi asimetri lain dan sulit untuk diretas karena perkalian skalarnya sulit untuk diimplementasikan.

Hill cipher yang umum digunakan hanya dapat menggunakan matriks persegi $n \times n$ sebagai kuncinya karena matriks $n \times n$ merupakan matriks yang *invertible* (memiliki invers). Namun, matriks persegi panjang $m \times n$ ternyata dapat menjadi suatu matriks yang *invertible* dengan memanfaatkan *pseudo-inverse*. Hidayat dan Alawiyah (2013) mengemukakan bahwa *hill cipher* dapat menggunakan matriks persegi panjang $m \times n$, dengan $m > n$ dan $n > 1$ sebagai kuncinya dengan memanfaatkan matriks *pseudo-inverse*. Cara ini berhasil meningkatkan tingkat keamanan kriptosistem karena kemungkinan matriks yang dapat dijadikan kunci kriptografi menjadi lebih luas. *Elliptic curve cryptography* umumnya digunakan untuk menyamarkan pesan berupa titik-titik pada kurva eliptik. Kumar, Suneetha & ChandrasekhAR (2012) mengimplementasikan *elliptic curve cryptography* untuk menyamarkan *plaintext* berupa teks. *Ciphertext* yang dihasilkan pun berupa teks sehingga sulit untuk mengetahui bahwa kriptosistem yang digunakan adalah *elliptic curve cryptography*, karena pada umumnya *elliptic curve cryptography* menghasilkan *ciphertext* berupa titik-titik pada kurva eliptik.

Agrawal dan Gera (2014) telah membahas bahwa penggunaan kriptosistem *hill cipher* yang digabungkan dengan *elliptic curve cryptography* berhasil meningkatkan keamanan dan meningkatkan kecepatan serta mengurangi memori yang dibutuhkan untuk melakukan kriptografi. Dalam penelitian tersebut, algoritma *hill cipher* yang digunakan berupa kunci matriks persegi $n \times n$ dan *ciphertext*nya berupa titik-titik pada kurva eliptik.

Dalam penelitian ini dilakukan pengembangan dari peningkatan keamanan dengan menggunakan kriptosistem *hill cipher* yang digabungkan dengan *elliptic curve cryptography*. Algoritma *hill cipher* yang digunakan memiliki kunci matriks persegi panjang $m \times n$, dengan $m \geq n$, $n > 1$ serta *plaintext* dan *ciphertext* yang digunakan berupa 95 karakter yang terdapat pada tabel ASCII dimulai dari karakter ke-32 sampai ke-126. Untuk mempermudah proses perhitungan dalam pembangkit kunci, enkripsi, dan dekripsi maka penulis membuat program aplikasi komputernya menggunakan *MATLAB*.

1.2 Batasan Masalah

Batasan masalah yang ada dalam penelitian ini adalah:

1. *Plaintext* berupa karakter alfanumerik yang selanjutnya dikonversi menjadi bilangan desimal pada tabel ASCII dimulai dari karakter ke-32 sampai ke-126.
2. Pada proses enkripsi dan dekripsi kriptosistem *hill cipher* menggunakan modulo 95, artinya inputan data ada 95 karakter.
3. Kunci *hill cipher* berupa matriks persegi panjang $m \times n$, dengan $m \geq n$ dan $n > 1$.
4. Kurva eliptik yang digunakan adalah kurva eliptik pada lapangan $\mathbb{Z}_p$ yang memiliki 95 titik.

1.3 Rumusan Masalah

Berdasarkan latar belakang masalah di atas maka diambil perumusan masalah sebagai berikut:

1. Bagaimana pengembangan kriptografi yang diperoleh dari penggabungan kriptosistem *hill cipher* dengan kunci matriks persegi panjang dan *elliptic curve cryptography*?
2. Bagaimana mengonstruksi program aplikasi komputer untuk mempermudah proses pembangkitan kunci, enkripsi, dan dekripsi

kriptosistem gabungan modifikasi *hill cipher* dan *elliptic curve cryptography* yang telah dikembangkan?

1.4 Tujuan Penelitian

Tujuan yang hendak dicapai dalam penelitian ini adalah:

1. Menggabungkan *hill cipher* dengan kunci matriks persegi panjang dan *elliptic curve cryptography*.
2. Mengonstruksi program aplikasi komputer untuk mempermudah proses pembangkitan kunci, enkripsi, dan dekripsi kriptosistem gabungan modifikasi *hill cipher* dan *elliptic curve cryptography* yang telah dikembangkan.

1.5 Manfaat Penelitian

Manfaat yang hendak dicapai dari penelitian ini adalah memberi kontribusi dalam bidang matematika terapan, khususnya aljabar terapan, melalui pengembangan kriptografi yaitu dengan menggabungkan modifikasi *hill cipher* dan *elliptic curve cryptography* untuk meningkatkan keamanan pesan rahasia berbantuan program *MATLAB*.

1.6 Sistematika Penulisan

Sistematika penulisan pada penelitian ini adalah sebagai berikut:

1. BAB I PENDAHULUAN

   Pada bab ini dijelaskan latar belakang penulisan, rumusan masalah, tujuan, dan manfaat yang ingin dicapai.
2. BAB II LANDASAN TEORI

   Pada bab ini dijelaskan teori dasar mengenai matriks, lapangan, kurva eliptik, kriptografi, *hill cipher*, *elliptic curve cryptography*, serta *software MATLAB* yang digunakan pada penelitian.
3. BAB III METODOLOGI PENELITIAN

Pada bab ini dijelaskan langkah-langkah yang dilakukan dalam menggabungkan *hill cipher* dengan kunci matriks persegi panjang dan *elliptic curve cryptography* serta rancangan program aplikasi komputer.

4. BAB IV PEMBAHASAN

   Pada bab ini dijelaskan hasil dan pembahasan penelitian.

5. BAB V KESIMPULAN DAN SARAN

   Pada bab ini diperoleh kesimpulan yang diperoleh dari penelitian dan beberapa saran untuk pengembangan selanjutnya.