BAB III

METODE PENELITIAN

Secara umum, dalam penelitian ini dikembangkan sebuah kriptosistem dengan cara menggabungkan *hill cipher* yang telah dimodifikasi sehingga kunci matriks yang digunakan berukuran $m \times n$ dan *elliptic curve cryptography* serta implementasi model ke dalam program komputer.

3.1 Perumusan Masalah

Semakin berkembangnya teknologi informasi dan komunikasi maka semakin banyak cara untuk mengkriptanalisis suatu pesan rahasia. Contohnya adalah kriptosistem *hill cipher* yang sudah dapat dikriptanalis dengan metode *known-plaintext attack*. Padahal, kriptosistem *hill cipher* memiliki keamanan yang tinggi jika dikriptanalisis dengan metode *ciphertext only attack* karena sifat linearitasnya. Untuk meningkatkan keamanan tersebut dapat dilakukan dengan menggabungkan dua kriptosistem dan memperbanyak jumlah kemungkinan kuncinya. Dalam penelitian ini akan dilakukan penggabungan kriptosistem *hill cipher* yang sudah dimodifikasi sehingga dapat menggunakan kunci matriks persegi panjang agar jumlah kemungkinan kuncinya bertambah dengan *elliptic curve cryptography*.

3.2 Model Dasar

Model dasar yang digunakan adalah kriptosistem *hill cipher* yang telah dimodifikasi sehingga dapat memiliki kunci matriks persegi panjang dan *elliptic curve cryptography*. Dalam kriptosistem *hill cipher*, *plaintext* dikonversi ke dalam bentuk desimal ASCII kemudian dienkripsi sehingga diperoleh suatu *ciphertext*. Oleh *elliptic curve cryptography*, *ciphertext* yang telah diperoleh disembunyikan kembali ke dalam titik-titik pada kurva eliptik. *Ciphertext* hasil penggabungan dua

kriptosistem ini berbentuk titik-titik pada kurva eliptik yang dikonversi ke dalam bentuk karakter alfanumerik. Keamanan algoritma ini didasarkan pada tingkat kesulitan dalam mengkriptanalisis penggabungan kriptosistem *hill cipher* dan *elliptic curve cryptography* serta banyaknya jumlah kemungkinan kunci pada kriptosistem *hill cipher*.

3.3 Pengembangan Kriptosistem *Hill Cipher* dengan Kunci Matriks Persegi Panjang dan *Elliptic Curve Cryptography*

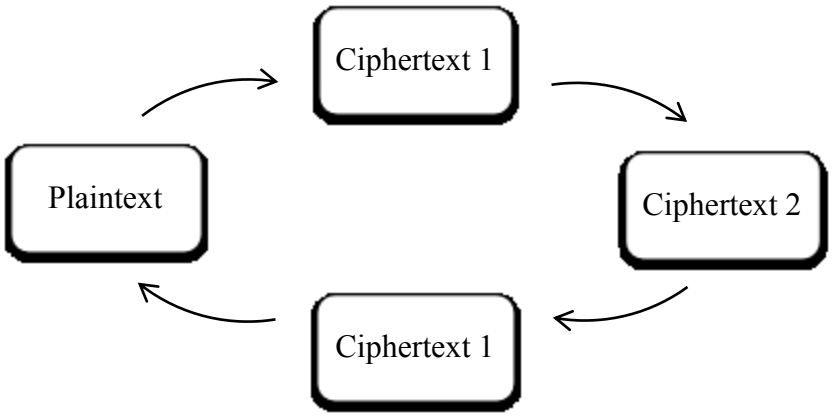
Pada penelitian ini akan dirancang sebuah kriptosistem gabungan antara kriptosistem *hill cipher* dan *elliptic curve cryptography* dengan kunci kriptosistem *hill cipher* adalah sebuah matriks persegi panjang. Tujuannya untuk meningkatkan keamanan kriptosistem gabungan tersebut dengan menambah kemungkinan matriks yang dapat dijadikan matriks kuncinya. *Plaintext* dan *ciphertext* berupa karakter alfanumerik yang terdapat pada tabel ASCII dimulai dari karakter ke-32 sampai ke-126. Langkah pertama adalah memilih matriks persegi panjang $m \times n$, dengan $m > n$ dan $n > 1$ yang memiliki invers semu (*pseudo-inverse*), menentukan E, yaitu titik-titik pada kurva eliptik atas lapangan $\mathbb{Z}_p$, dan generator dari E, serta menentukan kunci privat dan kunci publik untuk *elliptic curve cryptography*. Selanjutnya *plaintext* dienkripsi dengan kriptosistem *hill cipher* menggunakan matriks kunci. Hasil enkripsi tersebut akan dienkripsi kembali menggunakan *elliptic curve cryptography* sehingga diperoleh *ciphertext* berupa titik-titik pada kurva eliptik yang dikonversi ke dalam bentuk karakter alfanumerik untuk dikirimkan pada penerima pesan. Pada proses dekripsi, *ciphertext* yang diperoleh dari pengirim pesan didekripsi dengan *elliptic curve cryptography* menggunakan kunci privat dan kunci publiknya. Hasil dekripsi tersebut kemudian didekripsi lagi dengan kriptosistem *hill cipher* menggunakan *pseudo-inverse* dari matriks kunci sehingga diperoleh *plaintext*nya. Skema enkripsi dan dekripsi dapat dilihat pada gambar berikut:

Enkripsi menggunakan *hill cipher*

Enkripsi menggunakan *elliptic curve cryptography*

Dekripsi menggunakan

Dekripsi menggunakan *elliptic curve cryptography*



Gambar 3. 1 Skema proses enkripsi dan dekripsi

Untuk mempermudah proses pembangkitan kunci, enkripsi, dan dekripsi kriptosistem akan dilakukan pembuatan program komputer.

3.4 Konstruksi Program aplikasi komputer

Program penggabungan kriptosistem *hill cipher* dengan matriks kunci persegi panjang dan *elliptic curve cryptography* ini akan dibuat menggunakan *MATLAB*. Program tersebut bertujuan untuk memudahkan proses pembangkitan kunci, enkripsi, dan dekripsi. Rancangan program untuk kriptosistem ini memiliki tampilan awal (menu utama) yang memiliki tiga pilihan, yaitu pembangkitan kunci, enkripsi, dan dekripsi. Proses pembangkitan kunci adalah mengecek matriks persegi panjang yang dimiliki memenuhi syarat atau tidak, kemudian memilih kunci untuk *elliptic curve cryptography* dengan mencari E, yaitu titik-titik pada kurva eliptik atas lapangan $\mathbb{Z}_p$, serta menemukan generator dari E. Proses enkripsi membutuhkan inputan *plaintext*, kunci matriks, kurva eliptik, kunci privat, dan kunci publik *elliptic curve cryptography* dengan output *ciphertext*. Sementara untuk proses dekripsi membutuhkan inputan *ciphertext*, kunci matriks, kurva eliptik, kunci privat, dan kunci publik *elliptic curve cryptography*.

3.5 Validasi

Validasi dilakukan untuk mengetahui apakah *ciphertext* hasil proses enkripsi penggabungan kriptosistem *hill cipher* dengan kunci matriks persegi panjang dan *elliptic curve cryptography* dapat mengembalikan *plaintext* saat melalui proses dekripsi atau tidak.

3.6 Menarik Kesimpulan

Hasil dari penggabungan *hill cipher* dengan kunci matriks persegi panjang dan *elliptic curve cryptography* adalah sebuah kriptosistem yang memiliki keamanan lebih baik dan sukar untuk diretas, karena kriptanalis harus memecahkan dua kriptosistem dengan tingkat kesulitan tinggi untuk mendapatkan *plaintext* dari suatu *ciphertext*.