BAB III
METODE PENELITIAN

Berdasarkan penjelasan pada bab-bab sebelumnya, maka dapat dituliskan mengenai metode yang digunakan dalam penulisan skripsi ini.

2.1. Studi Literatur

Melalui studi literatur, dipelajari teori-teori yang berhubungan dengan kriptografi kurva *elliptic*, khususnya tentang algoritma ElGamal ECC. Sumbernya dapat berupa buku, artikel dan lain sebagainya.

2.2. Implementasi Program

Untuk memberikan hasil yang lebih nyata, maka perlu diimplementasikan kedalam sebuah program komputer yang dapat melakukan proses enkripsi dan dekripsi berdasarkan algoritma ElGamal ECC. Secara umum, langkah-langkah yang perlu dilakukan adalah

1. Proses Penentuan Kunci
   a. Menentukan bilangan bulat secara random $V \in [1, N_G - 1]$, dengan N_G adalah order dari *basic point* G_E(elemen pembangun grup *elliptic*).
   b. Menghitung *public key* $\beta = VG_E$.
   c. V adalah *private key* dan β *adalah public key.*
2. Proses Enkripsi
   a. Merepresentasikan *plaintext* menjadi titik kurva *elliptic* $P_{M.}$
   b. Memilih bilangan bulat secara random $k \in [1, N_G - 1]$.
   c. Mengenkripsi titik kurva *elliptic* P_M menjadi *chipertext pair of points* P_C dengan menggunakan *public key* penerima.
3. Proses Dekripsi
   a. Misalkan P_C adalah *chipertext pair of points* hasil enkripsi.

b. Titik pertama pada P_C dikalikan dengan *private key* penerima.
c. Hasil perkaliannya untuk mengurangi titik yang kedua pada P_C .
d. Menguraikan P_C sehingga dihasilkan titik kurva *elliptic* P_M.
e. Mengkonversi P_M menjadi menjadi *plaintext.*