BAB II
LANDASAN TEORI

2.1. Tinjauan Pustaka

Untuk menacapai tujuan penulisan skripsi, diperlukan beberapa pengertian dan teori yang relevan dengan pembahasan. Karena itu, dalam subbab ini akan diberikan beberapa teori yang berupa definisi maupun teorema yang relevan dengan pembahasan.

2.1.1. Grup Siklis

Sebelum diberikan definisi tentang grup siklis, terlebih dahulu dikemukakan mengenai pengertian grup, grup komutatif dan order dari grup.

Definisi 2.1 [Stallings, 2003:105] *Grup (G) adalah sebuah sistem aljabar yang terdiri dari suatu himpunan tak kosong G dan suatu operasi biner* (*) *yang didefinisikan dalam G serta memenuhi aksioma-aksioma berikut*

(*A1*) *Tertutup, yaitu jika* $a,b \in G$ *maka* $a * b \in G$.

(*A2*) *Assosiatif, yaitu* $a*(b*c) = (a*b)*c$, *untuk setiap* $a,b,c \in G$.

(*A3*) *Elemen identitas, yaitu terdapat elemen identitas 0 dalam G sedemikian sehingga* $a * 0 = 0 * a = a$, *untuk setiap* $a \in G$.

(*A4*) *Elemen invers. Untuk setiap a dalam G, terdapat a' elemen G sedemikian sehingga* $a * a' = a' * a = 0$.

Definisi 2.2 [Stallings, 2003:105] *Sebuah Grup G disebut sebagai grup komutatif jika memenuhi aksioma berikut*

(*A5*) *Komutatif, yaitu* $a * b = b * a$, *untuk setiap a,b dalam G.*

Definisi 2.3 [Stallings,2003:105] *Jika sebuah grup G memiliki jumlah elemen yang berhingga maka disebut grup berhingga (finite group) dan jika jumlah elemen dari suatu grup G tak berhingga maka disebut grup tak berhingga (infinite group). Order dari sebuah grup G sama dengan banyaknya elemen dalam grup G.*

ElGamal ECC bekerja dalam operasi aritmetika yang didefinisikan dalam suatu grup tertentu. Grup yang digunakan merupakan grup komutatif dan

berhingga. Sifat komutatif harus dipenuhi untuk menjamin bahwa *plaintext* yang dienkripsi dapat dikembalikan lagi atau dapat didekripsi. Selain itu juga perlu diketahui definisi dari grup siklis dan elemen pembangunnya, yaitu

Definisi 2.4 [Stallings,2003:106] *Sebuah grup G dan sebuah unsur* $g \in G$, *jika* $G=\{ g^n / n \in Z \}$ *maka G disebut sebagai grup siklis (cyclic group). Elemen g disebut elemen pembangun dari grup G.*

Algortima ElGamal ECC memerlukan beberapa parameter domain yang akan digunakan dalam proses enkripsi dan dekripsi. Salah satu parameter tersebut adalah elemen pembangun dari grup siklis yang digunakan dalam ElGamal ECC. Karena itu Definisi 2.4 diperlukan sebagai dasar teori dalam penulisan skripsi ini.

2.1.2. Lapangan Berhingga

Sebelum diberikan definisi tentang lapangan berhingga, terlebih dahulu diberikan definisi tentang gelanggang, gelanggang komutatif, daerah integral dan lapangan.

Definisi 2.5 [Stallings, 2003: 106] *Gelanggang* (*R*) *adalah sebuah sistem aljabar yang dibentuk oleh suatu himpunan tak kosong R, dua operasi biner yaitu penjumlahan* (+) *dan perkalian* (**.**) *yang didefinisikan dalam R , dan memenuhi aksioma-aksioma berikut*

(A1 – A5) *R adalah grup komutatif terhadap operasi penjumlahan.*

(*M1*) *Tertutup terhadap perkalian, yaitu jika* $a,b \in R$ *maka a.b dalam R.*

(*M2*) *Assosiatif terhadap perkalian, yaitu* $a.(b.c) = (a.b).c$ *, untuk setiap a,b,c dalam R.*

(*M3*) *Distributif, yaitu* $a.(b+c) = a.b + a.c$ *, untuk setiap a,b,c dalam R,*

$(a+b).c = a.c + b.c$ *, untuk setiap a,b,c dalam R.*

Definisi 2.6 [Stallings, 2003: 106] *Sebuah gelanggang R disebut sebagai gelanggang komutatif jika memenuhi aksioma berikut*

(M4) Komutatif terhadap perkalian, yaitu $a.b = b.a$ *, untuk setiap a,b dalam R.*

Definisi 2.7 [Stallings, 2003: 107] *Daerah integral merupakan suatu gelanggang komutatif R yang memenuhi aksioma-aksioma berikut*

(*M5*) *Identitas perkalian, yaitu terdapat* $1 \in R$ *sedemikian sehingga untuk setiap a*

anggota $\mathbb{R}$ *berlaku* $1.a = a.1 = a$.

(*M6*) *Tidak memuat pembagi nol, yaitu jika a, b dalam R dan* $a.b = 0$ *maka* $a=0$ *atau* $b=0$, *dimana 0 merupakan identitas penjumlahan.*

Berdasarkan Definisi 2.7, dapat dibentuk suatu lapangan dengan menambahkan satu aksioma, yaitu invers perkalian. Berikut ini, definisi dari lapangan dan lapangan berhingga.

Definisi 2.8 [Stallings, 2003: 107] *Lapangan* (F) *adalah sebuah sistem aljabar yang dibentuk oleh suatu himpunan tak kosong F dan dua operasi biner yaitu penjumlahan* (+) *dan perkalian* (**.**) *yang didefinisikan dalam F serta memenuhi aksioma-aksioma berikut*

(A1 – M6) F merupakan daerah integral.

(*M7*) *Invers perkalian, yaitu untuk setiap a dalam F dan* $a \neq 0$, *terdapat* $a^{-1} \in F$ *sedemikian sehingga* $a.\ a^{-1} = a^{-1}.a = 1$, *dengan 0 merupakan identitas dari penjumlahan dan 1 merupakan identitas perkalian.*

Definisi 2.9 [Certicom, 2000, SEC2: 3] *Jika sebuah lapangan F memiliki jumlah elemen yang berhingga maka F disebut lapangan berhingga (finite field) dan jika banyaknya elemen dalam lapangan F tak berhingga maka F disebut lapangan tak berhingga (infinite field).*

Proses perhitungan dalam ElGamal ECC menggunakan operasi aritmetika yang berlaku dalam suatu lapangan berhingga. Berdasarkan batasan masalah, lapangan yang digunakan dalam penulisan skripsi ini adalah lapangan berhiingga prima (F_p). Karena itu perlu diketahui pengertian dari lapangan F_p.

2.1.3. Lapangan Berhingga Prima (F_p)

Operasi aritmetika dalam F_p merupakan operasi modulo *p.* Sehingga perlu diketahui definisi dari modulo *p.*

Definisi 2.10 [Stinson, 1995: 3] *Misalkan s dan t bilangan bulat, dan p bilangan bulat positif. Maka dapat dituliskan* $s \equiv t \pmod p$ *jika p membagi* $t - s$. $s \equiv t \pmod p$ *dibaca "s kongruen t modulo p". Bilangan bulat positif p disebut modulus.*

Setelah diketahui berbagai definisi yang diperlukan, termasuk definisi modulo *p*, berarti telah dimiliki dasar yang cukup untuk mendefinisikan lapangan berhingga prima (F_p).

Definisi 2.11 [Certicom, 2000, SEC1: 3] *Lapangan berhingga prima F_p adalah suatu lapangan berhingga yang berisi p elemen. Anggota-anggota dari F_p direpresentasikan sebagai himpunan bilangan bulat dari 0 sampai p-1 atau ditulis {0,1,2,...p-1} dengan operasi penjumlahan dan perkalian yang didefinisikan sebagai berikut*

a. *Operasi penjumlahan, yaitu jika $a,b \in F_p$, maka $a + b = r$ dalam F_p, dengan $r \in [0,p-1]$ adalah sisa pembagian dari bilangan bulat a+b dibagi dengan p. Operasi tersebut dinamakan operasi penjumlahan modulo p dan ditulis: $a + b = r \pmod p$.*
b. *Operasi perkalian, yaitu jika $a,b \in F_p$, maka $a.b = s$ dalam F_p, dengan $s \in [0,p-1]$ adalah sisa pembagian dari bilangan bulat a.b dibagi dengan p. Operasi ini disebut sebagai operasi perkalian modulo p dan ditulis: $a.b = s \pmod p$.*
c. *Invers penjumlahan, yaitu jika $a \in F_p$, maka b invers dari a dalam F_p adalah solusi unik untuk persamaan $a + b = 0 \pmod p$.*
d. *Operasi perkalian, yaitu jika $a \in F_p$, maka b invers dari a dalam F_p adalah solusi unik untuk persamaan $a.b = 1 \pmod p$.*

Dalam representasi dari F_p ini, elemen identitas penjumlahan adalah 0 dan elemen identitas perkalian adalah 1.

2.1.4. Grup Elliptic atas F_p

ElGamal ECC merupakan algoritma kriptografi yang menggunakan permasalahan matematis ECDLP. Kurva *elliptic* dapat dipandang sebagai suatu himpunan yang terdiri dari titik-titik kurva *elliptic* atas F_p. Berikut ini, definisi tentang kurva *elliptic* atas F_p.

Definisi 2.12 [Certicom, 2000, SEC1: 6] *Misalkan F_p adalah sebuah lapangan berhingga prima sedemikian sehingga p adalah bilangan prima ganjil, dan $A,B \in F_p$ yang memenuhi $4A^3+27B^2 \neq 0 \pmod p$. Kurva elliptic $E(A,B)$ atas*

*F_p didefinisikan dengan parameter-parameter $A,B \in F_p$ yang berisi himpunan titik-titik (x,y) dengan $x,y \in F_p$ dan merupakan himpunan penyelesaian dari persamaan $y^2 \equiv x^3+Ax+B \pmod p$, termasuk titik **O** (point at infinity). Persamaan $y^2 \equiv x^3+Ax+B \pmod p$ disebut sebagai definisi persamaan dari Kurva Elliptic $E(F_p)$ atau sering ditulis $E(A,B)$.*

Definisi 2.13 [Stinson, 1995: 184] *Misalkan p > 3 adalah prima. Kurva elliptic $y^2=x^3+Ax+B$ atas F_p adalah himpunan penyelesaian $(x,y) \in F_p \times F_p$ dari*

$$y^2 \equiv x^3+Ax+B \pmod p$$

*dengan $A,B \in F_p$ adalah konstan, sedemikian sehingga $4A^3+27B^2 \neq 0 \pmod p$, termasuk titik khusus **O** yang disebut sebagai **point at infinity**.*

Berdasarkan Definisi 2.12 dan 2.13, dapat dibentuk suatu grup *elliptic* atas F_p. Sebagai dasar teori dalam grup *elliptic*, terlebih dahulu diberikan definisi tentang *quadratic residue modulo p.*

Definisi 2.14 [Stinson, 1995: 313] *Misalkan p adalah bilangan prima ganjil dan x bilangan bulat, $0 \leq x \leq p-1$. Bilangan x didefinisikan sebagai suatu **quadratic residue** modulo p (QR_p), jika kongruensi $y^2 \equiv x \pmod p$ mempunyai suatu penyelesaian $y \in F_p$. Jika $x \neq 0 \pmod p$ dan x bukan quadratic residue modulo p maka x didefinisikan sebagai **quadratic non-residue** modulo p.*

Sehingga dapat didefinisikan grup *elliptic* atas F_p sebagai berikut

Definisi 2.15 [Chouinard, 2002: 1] *Sebuah grup elliptic $E_p(A,B)$ atas F_p diperoleh dengan menghitung penyelesaian persamaan $y^2 \equiv x^3+Ax+B \pmod p$ untuk $0 \leq x \leq p-1$, A dan $B \in F_p$, p bilangan prima, sehingga memenuhi syarat : $4A^3 + 27B^2 \neq 0 \pmod p$ dan y^2 merupakan anggota himpunan quadratic residue modulo p (QR_p) termasuk didalamnya titik **O** (point at infinity).*

Sebagaimana dijelaskan sebelumnya bahwa ElGamal ECC bekerja dalam suatu grup tertentu. Grup yang dimaksud adalah grup *elliptic* $E_p(A,B)$ atas F_p dan operasi aritmetika yang berlaku didalamnya.

2.1.5. Public Key Cryptosystem

ElGamal ECC merupakan salah satu jenis *public key cryptosystem*. Karena itu, perlu diketahui terlebih dahulu tentang pengertian *cryptosystem* dan *public key*

cryptosystem.

Definisi 2.16 [Stinson, 1995: 1] *Cryptosystem terdiri atas 5-tuple, yaitu (M, C_k, K, E_k, D_k) yang memenuhi pengertian sebagai berikut*

a. *M adalah himpunan berhingga dari plaintext.*
b. *C_k adalah himpunan berhingga dari chipertext.*
c. *K adalah himpunan berhingga dari kunci.*
d. *Untuk setiap $k \in K$ terdapat aturan kunci enkripsi $e_k \in E_k$ dan berkorespondensi dengan aturan kunci dekripsi $d_k \in D_k$. Untuk setiap $e_k : M \to C_k$ dan $d_k : C_k \to M$ adalah suatu fungsi sedemikian sehingga $d_k(e_k(x)) = x$, untuk setiap x dalam M.*

Definisi 2.17 [Stallings, 2003: 260] *Skema enkripsi pada public key cryptosystem mempunyai 6 unsur, yaitu:*

a. *Plaintext adalah data atau pesan yang dapat dibaca.*
b. *Algoritma enkripsi adalah algoritma untuk membuat plaintext menjadi kode-kode tertentu (chipertext).*
c. *Public key adalah kunci yang digunakan untuk enkripsi.*
d. *Private key adalah kunci yang digunakan untuk dekripsi.*
e. *Chipertext adalah data atau pesan hasil enkripsi dari plaintext.*
f. *Algoritma dekripsi adalah algoritma untuk membuat chipertext menjadi plaintext.*

2.2. Kerangka Pemikiran

Berdasarkan latar belakang masalah dan landasan teori yang telah diberikan, dapat disusun suatu kerangka pemikiran penulisan skripsi ini. Dengan alasan kerahasiaan, sebuah informasi (*plaintext*) yang disampaikan dari sumber berita perlu disandikan agar tidak dapat diketahui atau dibaca oleh orang-orang yang tidak berhak atau tidak bertanggungjawab. Kriptografi dapat digunakan untuk mengenkripsi *plaintext* menjadi teks yang disandikan (*ciphertext)*.

Langkah pertama adalah menentukan *private key* $V < N_G - 1$, dengan N_G adalah order dari *basic point* G_E (elemen pembangun dalam grup *elliptic*),

sehingga $N_G . G_E = \boldsymbol{O}$ *(point at infinity)*. Selanjutnya, menghitung *public key* $\beta = VG_E$, dengan G_E adalah *basic point* dan G_E anggota grup *elliptic* $E_p(A, B)$ atas F_p.

Sebelum melakukan enkripsi, *plaintext* direpresentasikan terlebih dahulu menjadi titik kurva *elliptic* (P_M) yang merupakan elemen dalam $E_p(A,B)$. Misalkan Bob ingin mengirim kepada Iwan sebuah *plaintext* yang telah direpresentasikan sebagai titik kurva *elliptic* P_M . Bob memilih sebuah bilangan bulat k secara random dan menghitung *chipertext pair of points* $P_C (P_1, P_2)$ menggunakan *public key* Iwan (β).

$$P_1 = k . G_E \qquad dan \qquad P_2 = P_M + k . \beta .$$

Setelah menerima *chipertext* tersebut, Iwan perlu mendekripsi *chipertext pair of points* (P_C) untuk mendapatkan *plaintext*.

Untuk mendekripsi *chipertext*, Iwan mengalikan titik pertama pada *chipertext pair of points* (P_1) dengan *private key* miliknya (V). Kemudian mengurangi titik kedua *chipertext pair of points* (P_2) dengan hasil perkalian antara titik pertama dan *private key*. Sehingga diperoleh pesan aslinya yang berupa titik P_M seperti berikut

$$(P_M + k\beta) - [V (kG_E)] = (P_M + kV G_E) - [V (k G_E)] = P_M$$

Kemudian titik kurva *elliptic* P_M dikonversi menjadi *plaintext*, sehingga Iwan dapat mengerti pesan yang dikirim oleh Bob.