KRIPTOGRAFI KURVA ELIPTIK ATAS LAPANGAN GALOIS PRIMA $GF(p)$ DENGAN BASIS 95

Annisa Nur Azizah[1)], Solichin Zaki[2)], Nikken Prima Puspita[3)].
[1] FSM, Universitas Diponegoro
email: annisazizah20@gmail.com
[2] FSM, Universitas Diponegoro
[3] FSM, Universitas Diponegoro

Abstrak

Kriptografi kurva eliptik adalah sistem kriptografi yang termasuk kedalam kriptografi kunci publik. Kriptosistem ini didefinisikan pada lapangan berhingga yang disebut lapangan Galois. Lapangan Galois yang elemennya direpresentasikan dalam modulo prima disebut lapangan Galois prima $GF(p)$. Himpunan titik-titik yang terbentuk dari kurva eliptik membentuk suatu grup berhingga yang digunakan untuk tingkat keamanan dalam kriptografi yang disebut ECDLP (*Elliptic Curve Discret Logarithm Problem*). Semakin besar bilangan prima, maka tingkat keamanan pesan dengan menggunakan sistem kriptografi kurva eliptik atas $GF(p)$ semakin tinggi. Pembahasan algoritma kriptografi kurva eliptik atas $GF(p)$ dibagi menjadi proses pembentukan kunci, proses enkripsi dan proses dekripsi. Ketiga proses ini berbentuk titik, yang generator awalnya diambil dari sebuah grup eliptik. Kriptografi disini menggunakan basis 95, yaitu mendefinisikan karakter ASCII sebanyak 95 karakter. Proses pembentukan kunci yang terdiri dari kunci publik dan kunci privat. Hal terpenting dalam proses pembentukan kunci adalah menentukan titik generator G dari grup eliptik atas $GF(p)$. Setelah kunci publik didapatkan maka kunci dikirim kepada pengirim untuk proses enkripsi. Proses enkripsi menggunakan algoritma enkripsi kriptografi kurva eliptik, dengan pesan dikonversikan kedalam bilangan ASCII yang hasil cipherteksnya berbentuk sebuah titik. Setelah menghasilkan cipherteks, maka pengirim mengirimkan pesan cipherteks kepada penerima. Kemudian penerima pesan melakukan proses dekripsi dengan kunci privat. Proses dekripsi menggunakan algoritma dekripsi kriptografi kurva eliptik yang akhirnya menghasilkan plainteks dan plainteks dikonversikan menjadi pesan asli.

Kata Kunci: kurva eliptik, kriptografi kurva eliptik, lapangan Galois prima, enkripsi, dekripsi.

Abstract

Elliptic curve cryptography is a cryptographic system which belongs to public-key cryptography. Cryptosystem is implemented on a finite field known as Galois field. A Galois field in which the elements are represented in modulo prime is called as prime Galois field $GF(p)$. A set of dotted which is made from elliptic curve forms a finite group that is used for its level of security in cryptography is called as ECDLP (Elliptic Curve Discret Logarithm Problem). The greater the prime number, the higher level of security would be applied on the cryptography system of upper curve elliptic $GF(p)$. This discussion on algorythm on upper elliptic curve cryptography $GF(p)$ in the process of making a key, encryption and decryption. The third process is shaped dots, he generator was originally taken from a group of elliptic. In this cryptography use base 95, which defines the ASCII characters as many as 95 characters. The process of making a key comprises public key and private key. Encryption process uses algorithms of elliptic curve cryptography encryption, by converting the message into ASCII number in which the ciphertext is in a form of a dot. After get a ciphertext the sender sends the chipertext message to the receiver. Afterthat receiver do decryption process using a private key. Algorithm of elliptic curve criptography decryption is applied on the decryption process which eventually produces a plaintext. This plaintext is further converted into an original message.

Keywords: *elliptic curve, elliptic curve cryptography, Galois field prime, encryption, decryption.*

A. PENDAHULUAN

Perkembangan teknologi informasi dan komunikasi sangat cepat dan pesat, hal ini yang menyebabkan munculnya kemajuan teknologi informasi. Seiringnya perkembangan teknologi informasi, kejahatan dari teknologi informasi pun juga semakin banyak. Pesan informasi yang ingin disampaikan ke pihak yang lain menjadi tidak aman karena adanya penyadapan dari pihak ketiga yang tidak berhak atas pesan tersebut. Mereka merubah atau dengan sengaja yang menyebabkan pesan yang diterima tidak asli bahkan rusak. Salah satu cara untuk mempertahankan kerahasiaan dari pesan tersebut adalah menggunakan kriptografi. Sebagian pihak meginginkan pengamanan yang lebih kuat maka beberapa pihak menggunakan kriptografi kunci publik, yaitu sistem kriptografi yang memiliki 2 kunci. Sistem kriptografi RSA dan ElGamal merupakan sistem kriptografi kunci publik yang banyak dipakai namun

memiliki kelemahan, yaitu membutuhkan ukuran kunci yang besar. Pada tahun 1985 munculah kriptografi yang dikembangkan oleh Victor Miller dan Neal Koblitz, yaitu kriptografi kurva eliptik. Penggunaan kriptografi kurva eliptik lebih efisien dibandingkan dengan kriptosistem yang sudah ada, seperti RSA dan ElGamal, karena ukuran kunci yang lebih kecil namun memperoleh derajat keamanan yang setara. Keuntungan ukuran kunci lebih kecil adalah waktu perhitungan yang lebih cepat dan memori yang diperlukan lebih kecil.

Kriptografi ini didasari oleh struktur aljabar yakni pemetaan, himpunan, grup, ring, dan lapangan. Lapangan berhingga disebut juga lapangan Galois. Perhitungan dalam kriptografi ini menggunakan dasar dari teori bilangan, antara lain pembagian, bilangan prima, pengujian bilangan prima, dan algoritma perluasan Euclid untuk mencari invers modulo.

Kriptografi kurva eliptik menggunakan basis kurva eliptik. Kurva eliptik dalam kriptografi tidak mempunyai solusi dalam bilangan riil. Akibatnya agar kurva eliptik mempunyai solusi di dalam kriptografi, maka kurva eliptik didefinisikan dalam lapangan Galois yaitu lapangan berhingga prima dan lapangan berhingga biner.

Pembahasan dalam makalah ini adalah bagaimana menggunakan algoritma kurva eliptik atas lapangan Galois prima. Kriptografi kurva eliptik akan mengenkripsi dan mendekripsi dengan basis titik. Titik tersebut berawal dari generator yang diambil sebarang dari grup eliptik. Karena basis pada kriptografi kurva eliptik ini adalah titik, maka kelebihan dari kriptografi ini adalah kunci lebih kecil. Kunci yang lebih kecil membutuhkan memori yang kecil dan proses yang dibutuhkan juga semakin sedikit.

B. METODE

Langkah-langkah yang dilakukan peneliti dalam penelitian ini adalah sebagai berikut.

1. Mengkaji teori-teori dasar kriptografi.
2. Menyajikan masalah *Elliptic Curve Cryptography* (ECC) atas lapangan Galois prima.
3. Menganalisa proses pembentukan kunci, proses enkripsi dan proses dekripsi menggunakan algoritnma kriptografi kurva eliptik
4. Mengambil kesimpulan.

C. HASIL DAN PEMBAHASAN

Algoritma kriptografi kurva eliptik adalah teknik kriptografi yang didasarkan pada pendekatan matematika dengan menggunakan kurva eliptik. Tingkat keamanan sistem kriptografi kurva eliptik didasarkan atas ECDLP pada kurva eliptik modulo prima. Semakin besar bilangan prima dan ECDLP yang digunakan, maka tingkat keamanan pengiriman pesan dengan menggunakan sistem kriptografi kurva eliptik semakin tinggi. Kriptografi kurva eliptik (*Elliptic Curve Cryptography)* menggunakan dua kunci yaitu kunci publik dan kunci privat. Kunci publik pada kriptografi kurva eliptik adalah sebuah titik pada kurva eliptik dan kunci privatnya adalah sebuah angka acak. Kunci publik diperoleh dengan melakukan operasi perkalian terhadap kunci privat dengan titik generator G pada kurva eliptik. Titik generator G didapatkan dari memilih acak titik pada grup eliptik. Operasi titik pada kriptografi kurva eliptik tidak mengoperasikan titik seperti biasa, namun ada operasi khusus yang digunakan. Sebelum menjabarkan operasi titik akan dijabarkan terlebih dahulu tentang mencari invers modulo dengan algoritma perluasan Euclid.

Algoritma Perluasan Euclid

Salah satu penggunaan Algoritma perluasan Euclid atau yang sering disebut dengan algoritma *extended Euclid* adalah untuk mencari invers modulo. Invers modulo terjadi jika $a \in \mathbb{Z}_n$ maka nilai $\gcd(a,n) = 1$. Invers modulo digunakan dalam perhitungan operasi titik dalam kriptografi kurva eliptik.

Berikut diberikan langkah-langkah dari Algoritma perluasan Euclid dan penyajian algoritma dalam bentuk tabel sebagai berikut.

Tabel 1. Invers modulo dengan perluasan Euclid

Q	R_1	R_2	R	T_1	T_2	T
..	..	..	..	..	..	..

Keterangan:

$Q =$ hasil bagi antara R_1 dibagi R_2

$R_1 =$ nilai awal modulo, untuk selanjutnya didapatkan dari nilai R_2 baris sebelumnya

$R_2 =$ nilai awal pembagi/penyebut, untuk selanjutnya didapatkan dari nilai R baris sebelumnya

$R =$ sisa dari R_1 dibagi R_2

$T_1 = 0$ pada awal, untuk selanjutnya didapatkan dari nilai T_2 baris sebelumnya

$T_2 = 1$ pada awal, untuk selanjutnya didapatkan dari nilai T baris sebelumnya

$T = T_1 - Q \cdot T_2$

Berikut diberikan langkah-langkah algoritma perluasan Euclid untuk mencari invers modulo.

Langkah-langkah mencari invers $\boldsymbol{b \bmod a}$:

1. Memasukkan nilai a dan b berturut-turut sebagai R_1 dan R_2
2. Memasukkan nilai $T_1 = 0, T_2 = 1$
3. Menghitung nilai Q, yaitu hasil bagi R_1/R_2
4. Menghitung nilai R, yaitu $R_1 - Q \cdot R_2$ atau sisa dari R_1/R_2
5. Menghitung nilai T, yaitu $T_1 - Q \cdot T_2$
6. Tahap selanjutnya, nilai R_1 didapat dari nilai R_2 sebelumnya dan nilai R_2 didapat dari nilai R sebelumnya
7. Nilai T_1 didapat dari nilai T_2 sebelumnya dan nilai T_2 didapat dari nilai T sebelumnya.
8. Selanjutnya menghitung Q, R, T seperti langkah sebelumnya
9. Jika $R > 0$ maka mengulangi langkah 6 sampai 8
10. Jika $R = 0$ maka berhenti dan menetapkan T_2 sebagai invers.

Contoh 1.
Mencari invers dari $7 \ mod \ 11$, dengan $a = 11$ dan $b = 7$.
Dengan menggunakan tabel perluasan Euclid, maka dapat dilihat iterasinya sebagai berikut

Tabel 2. Mencari invers $7 \ mod \ 11$ dengan perluaan Euclid

Q	R_1	R_2	R	T_1	T_2	T
1	11	7	4	0	1	10
1	7	4	4	1	10	2
1	4	3	1	10	2	8
3	3	1	0	2	**8**	0

Karena $R = 0$, maka iterasi berhenti dan didapatkan nilai $\boldsymbol{T_2 = 8}$. Jadi invers $7 \ mod \ 11$ adalah 8.

Lapangan Galois

Diberikan definisi dari lapangan Galois.

Definisi 1. *Lapangan Galois adalah lapangan berhingga yang mempunyai order p^n, ditulis dengan $GF(p^n)$.*

$\mathrm{GF(p^n)}$ dimana p prima dan n bilangan bulat positif. GF adalah singkatan dari lapangan Galois, menghormati matematikawan yang pertama mempelajari mengenai lapangan berhingga.

Selanjutnya pada $GF(p^n)$ ada 2 hal khusus yang digunakan, yaitu $n = 1$ dan $p = 2$. Jika $n = 1$, diperoleh lapangan Galois $GF(p)$, yang disebut juga sebagai lapangan Galois prima. Sedangkan jika $p = 2$, diperoleh lapangan Galois $GF(2^n)$, yang disebut juga sebagai lapangan Galois biner atau lapangan Galois berkarakteristik dua. Dalam pembahasan ini dibahas hanya untuk lapangan Galois prima $GF(p)$.

Diberikan definisi dari lapangan Galois prima.

Definisi 2. *Galois field prima $GF(p)$ adalah suatu lapangan berhingga yang berisi p elemen*.

$GF(p)$ terdiri dari himpunan bilangan $\mathbb{Z}_p$ dengan p bilangan prima. Berikut diberikan definisi elemen-elemen dari $GF(p)$ dan operasinya.

Definisi 3 *Untuk setiap bilangan prima, $GF(p) = \{0,1, \dots, p-1\}$ dengan operasi penjumlahan dan perkalian yang sebagai berikut*

a. *Operasi penjumlahan*
   Untuk setiap $a, b \in GF(p)$, berlaku $a + b \in GF(p)$.
b. *Operasi perkalian*
   Untuk setiap $a, b \in GF(p)$, berlaku $a \cdot b \in GF(p)$.
c. *Invers penjumlahan*
   Untuk setiap $a \in GF(p)$, maka $(-a)$ invers dari a, $-a \in GF(p)$ adalah solusi tunggal untuk persamaan $a + x \equiv 0 \ (mod \ p)$
d. *Invers perkalian*
   Untuk setiap $a \in GF(p)$ dengan $a \neq 0$, maka a^{-1} adalah invers dari a,
   $a^{-1} \in GF(p)$ adalah solusi tunggal untuk persamaan $a.x \equiv 1 \ (mod \ p)$.

Grup Eliptik

Berikut diberikan definisi dari kurva eliptik.

Definisi 4. *Diberikan p bilangan prima dan misalkan $GF(p)$ dinotasikan sebagai lapangan atas bilangan bulat modulo p. Kurva eliptik E atas $GF(p)$ didefinisikan dengan persamaan*

$$y^2 \equiv x^3 + ax + b \ (mod \ p)$$

dimana $a, b \in GF(p)$ memenuhi $4a^3 + 27b^2 \not\equiv 0 \ (mod \ p)$.

Grup eliptik dapat dipandang sebagai suatu himpunan yang terdiri dari titik-titik kurva eliptik atas $GF(p)$. Pasangan (x, y) dimana $x, y \in GF(p)$ adalah titik pada kurva jika (x, y) memenuhi persamaan $y^2 \equiv x^3 + ax + b \ (mod \ p)$, termasuk di dalam kurva *point at infinity* yang dinotasikan dengan O. Himpunan semua titik pada E dinotasikan dengan $E\big(GF(p)\big)$ atau $E_p(a, b)$.

Berikut ini dijelaskan mengenai *quadratic residue* yang mendasari perhitungan dalam grup eliptik.

Definisi 5. *Diberikan $a \in \mathbb{Z}_n^*$. Bilangan a disebut quadratic residu modulo n atau akar kuadrat modulo n jika terdapat $x \in \mathbb{Z}_n^*$ sedemikian sehingga $x^2 \equiv a \ (mod \ n)$.*

Jika tidak ada nilai x yang memenuhi, maka a disebut *quadratic non-residu* modulo *n*. Himpunan dari semua *quadratic residu* modulo *n* dinotasikan dengan Q_n dan himpunan semua *quadratic non-residu* modulo *n* dinotasikan dengan $\overline{Q_n}$.

Akibatnya untuk setiap nilai x perlu diketahui merupakan *quadratic residu* atau *quadratic non-residu*. Jika x adalah *quadratic residu* maka diperoleh 2 elemen (y_1, y_2) dalam grup eliptik. Sedangkan jika x adalah *quadratic*

non-residu maka titik tidak berada dalam grup eliptik $E_p(a,b)$.

Operasi-Operasi titik

Berikut diberikan operasi penjumlahan yang didefinisikan
$P, Q \in E$ dengan P adalah titik (x_p, y_p) dan Q adalah titik (x_q, y_q).

i. Penjumlahan titik
$P + Q = R(x_r, y_r)$ dengan $x_p \neq x_q$ adalah sebagai berikut.

$$x_r = \lambda^2 - x_p - x_q$$
$$y_r = \lambda(x_p - x_r) - y_p$$

dimana,

$$\lambda = \frac{y_q - y_p}{x_q - x_p}$$

ii. Penggandaan titik
$2P = R(x_r, y_r)$ dengan $x_p = x_q$ dan $y_p = y_q$ adalah sebagai berikut.

$$x_r = \lambda^2 - 2x_p$$
$$y_r = \lambda(x_p - x_r) - y_p$$

dimana,

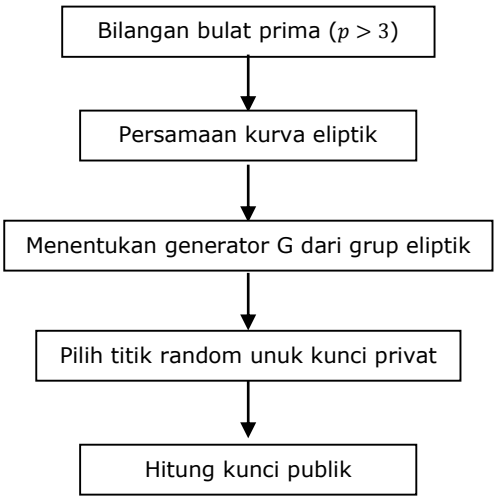
$$\lambda = \frac{3(x_p)^2 + a}{2y_p}$$

iii. Perkalian titik
Misalkan P adalah titik pada kurva eliptik. Operasi perkalian P adalah didefinisikan dengan penjumlahan yang berulang kali.

$$kP = P + P + P + \cdots + \ banyaknya\ k.$$

Algoritma Pembentukan Kunci

Langkah-langkah dalam pembentukan kunci dapat dilihat pada Gambar 1.



Gambar 1. Diagram pembentukan kunci kriptografi kurva eliptik

Dari Gambar 1 penulis dapat menjabarkan langkah-langkah sebagai berikut:

1. Menentukan bilangan prima (p) dengan syarat $p > 3$..
   Misalkan diambil p=17
2. Menentukan bentuk persamaan kurva eliptik.
   Misalkan dibuat kurva eliptik dengan, $a = 1, b = 1, p = 17$.
   Sehingga,
   $y^2 \equiv x^3 + (1)x + (1)\ (mod\ p)$
   $y^2 \equiv x^3 + x + 1\ (mod\ 17)$
   Diperiksa jika $a = 1, b = 1$ dan $p = 17$, maka $4a^3 + 27b^2 \not\equiv 0\ (mod\ p)$
   $4a^3 + 27b^2 = 4(1)^3 + 27(1)^2$
   $= 4 + 27$
   $= 31$
   $\equiv 14\ (mod\ 17)$
   Jadi persamaan $y^2 \equiv x^3 + x + 1\ (mod\ 17)$ merupakan persamaan kurva eliptik.
3. Menentukan titik generator G dari grup eliptik atas $GF(p)$
   Sebelum menentukan grup eliptik atau titik-titik $E_{17}(1,1)$, terlebih dahulu mencari *quadratic residu* Q_{17}

   Tabel 1. Tabel untuk mencari Q_{17}

$x^2\ (mod\ 17)$	Hasil
$1^2\ mod\ 11$	1
$2^2\ mod\ 11$	4
$3^2\ mod\ 11$	9
$4^2\ mod\ 11$	16
$5^2\ mod\ 11$	8
$6^2\ mod\ 11$	2
$7^2\ mod\ 11$	15
$8^2\ mod\ 11$	13
$9^2\ mod\ 11$	13
$10^2\ mod\ 11$	15
$11^2\ mod\ 11$	2
$12^2\ mod\ 11$	8
$13^2\ mod\ 11$	16
$14^2\ mod\ 11$	9
$15^2\ mod\ 11$	4
$16^2\ mod\ 11$	1

   Jadi himpunan $quadratic\ residu$ mod 17 adalah $Q_{17} = \{1, 2, 4, 8, 9, 12, 15, 16\}$. Kemudian menentukan elemen grup eliptik $E_{17}(1,1)$ yang merupakan penyelesaian dari persamaan $y^2 = x^3 + x + 1\ (mod\ 17)$ untuk $x \in GF(17)$ dan $y^2 \in Q_{17}$.
   Berikut tabel untuk mencari elemen grup eliptik $E_{17}(1,1)$.

Tabel 2. Tabel $E_{17}(1,1)$.

x	0	1	2	3	4	5
y^2	1	3	11	14	1	12
$y^2 \in Q_{17}$	*Ya*	*Tidak*	*Tidak*	*Tidak*	*Ya*	*Tidak*
y_1	1	–	–	–	1	–
y_2	16	–	–	–	16	–

x	6	7	8	9	10	11
y^2	2	11	11	8	8	0
$y^2 \in Q_{17}$	*Ya*	*Tidak*	*Tidak*	*Ya*	*Ya*	*Tidak*
y_1	6	–	–	5	5	–
y_2	11	–	–	12	12	–

x	12	13	14	15	16
y^2	7	1	5	8	16
$y^2 \in Q_{17}$	*Tidak*	*Ya*	*Tidak*	*Ya*	*Ya*
y_1	–	1	–	5	4
y_2	–	16	–	12	13

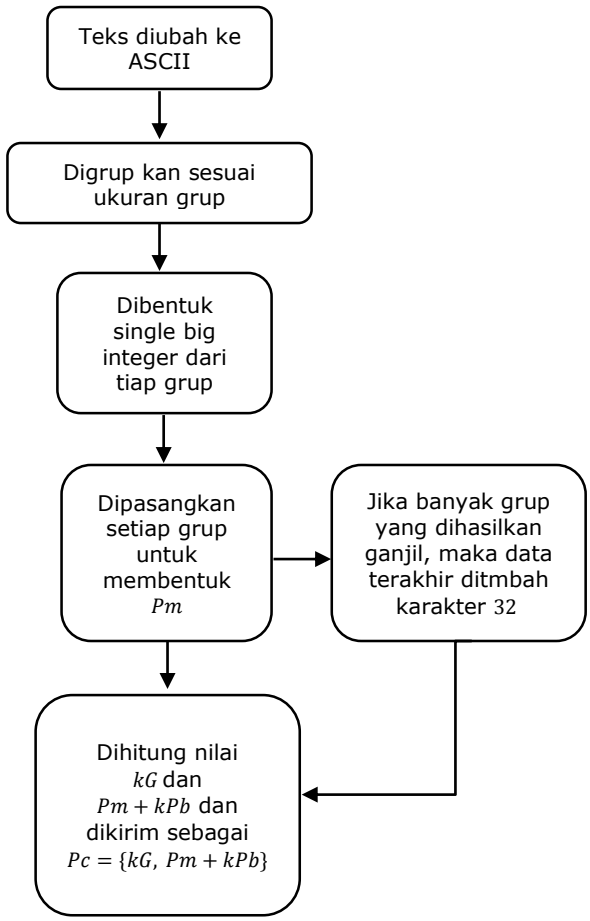
Grup eliptik $E_{11}(1,6)$ memuat titik:
$E_{17}(1,1) = \{(0,1), (0,16), (4,1), (4,16), (6,6), (6,11), (9,5), (9,12), (10,5), (10,12), (13,1), (13,16), (15,5), (15,12), (16,4), (16,13)\}$

Setelah itu, dipilih sebuah titik yang dijadikan titik generator, misalkan ambil titik $G = (6,11)$.

4. Menentukan kunci privat A dan kunci privat B
   Kunci privat $A = nA$
   Kunci privat $B = nB$
   Kunci privat A dan B ditentukan dengan nilai acak dimana nilai kunci tersebut merupakan elemen dari $nA, nB \in \{2, 3, \dots, p-1\}$ dalam $GF(p)$.
   Misalkan dipilih $nA = 2$ dan $nB = 3$.
5. Menghitung kunci publik A dan kunci publik B
   Kunci publik A $Pa = nA \cdot G$
   Kunci publik B $Pb = nB \cdot G$
   Kunci publik dihitung oleh masing-masing pengguna dengan melakukan operasi perkalian titik antara kunci privat masing-masing dengan titik G.
   Pengirim A dengan $nA = 2$ dan titik $G(2,7)$, maka :
   $Pa = nA \cdot G$
   $= 2 \cdot (6,11)$
   $= (6,11) + (6,11)$
   $= (9,12)$
   Jadi, kunci publik A adalah $Pa(9,12)$.
   Sedangkan untuk pengguna $B, nB = 7$, titik $G(6,11)$, maka :
   $Pb = nB \cdot G$
   $= 7 \cdot (9,12)$
   $= (6,11) + (6,11) + (6,11) + (6,11) + (6,11) + (6,11) + (6,11)$
   $= (9,12) + (9,12) + (9,12) + (6,11)$
   $= (16,14)$
   Jadi, kunci publik B adalah $Pb(16,14)$.

Algoritma Enkripsi ECC

Langkah-langkah dalam pembentukan kunci dapat dilihat pada Gambar 2.



Gambar 2. Diagram algoritma enkripsi kriptografi kurva eliptik

Dari Gambar 1 penulis dapat menjabarkan langkah-langkah sebagai berikut.

Input :

Mempersiapkan teks yang akan dikirim

Proses :

1. Mengkonversi teks kedalam nilai ASCII
   Setiap karakter yang ada dalam teks terlebih dahulu harus dikonversikan kedalam angka-angka yang bersesuain berdasarkan ASCII.
2. Menghitung nilai groupsize, yaitu ukuran grup/kelompok yang akan dipartisi.
   Group size mempunyai perintah/*command* berikut
   $group\ size = Length\left[IntegerDigits[p, 65536]\right] - 1$
   Perhitungan IntegerDigits adalah dengan cara mengkonversi bilangan prima p dengan basis 65536.
3. Mempartisi/membagi nilai ASCII menjadi beberapa kelompok.
   Keseluruhan dari nilai ASCII dibagi menjadi kelompok-kelompok yang setiap kelompok tersebut akan dirubah menjadi big integer. Dalam bantuan program Mathematica,

command untuk partisi adalah sebagai berikut

$Partition[ASCII\ values, group\ size, groupsize, 1, \{\}]$

Command partisi tersebut menyatakan bahwa nilai ASCII keseluruhan dipecah menjadi beberapa kelompok yang masing-masing kelompok berukuran $groupsize$.

$Groupsize$ dalam *command* yang pertama menyatakan bahwa banyaknya karakter pada setiap partisi ada sebanyak $groupsize$, dan *command* $groupsize$ selanjutnya menyatakan bahwa dalam setiap partisi terdapat sebanyak $groupsize$ karakter tanpa pengulangan di partisi selanjutnya. Karakter 1 dan $\{\}$ pada *command* menyatakan bahwa jika terdapat sisa dan tidak berukuran sebanyak $groupsize$ maka tidak membutuhkan adanya penambahan karakter dan sisa diletakkan pada partisi yang terakhir.

4. Masing-masing grup yang didapatkan dari langkah sebelumnya dikonversikan kedalam nilai bilangan bulat besar (*big integer*) yang berbasis 65536. Dalam program, *command* untuk konversi adalah

   $\text{FromDigits}[\text{Group of ASCII values}, 65536]$
5. Menambahkan dengan karakter 32 di akhir data dari langkah di atas jika banyaknya grup yang dihasilkan berjumlah ganjil, hal ini dilakukan untuk membentuk pasangan yang komplit. Menambahkan dengan nilai 32, karena dalam kode ASCII 32 merepresentasikan *blank space* atau spasi. Selanjutnya masing-masing pasangan menjadi input dalam system ECC sebagai "Pm" atau plainteks.
6. Memilih nilai k, dimana k adalah nilai acak antara kisaran 1 sampai $n-1$. Menghitung kG dan kPb menggunakan operasi perkalian titik.
7. Menghitung $\{Pm + kPb\}$ menggunakan penjumlahan titik atau penggandaan titik seperti yang dibutuhkan.
8. Menggabungkan titik $\{kG\}$ dan titik $\{Pm + kPb\}$ menjadi

   $Pc = \{kG, Pm + kPb\}$. Pc inilah yang menjadi cipherteks yang akan dikirim ke pihak penerima.

Output :

Cipherteks berupa titik dengan,

$Pc = \{kG, Pm + kPb\}$.

Algoritma Dekripsi ECC

Langkah-langkah pada proses dekripsi adalah sebagai berikut:

Input :

Cipherteks $Pc = \{kG, Pm + kPb\}$ yang telah diperoleh dari proses enkripsi

Proses :

1. Memisahkan Pc ke bagian kiri $\{kG\}$ dan bagian kanan $\{Pm + k\,P\,b\}$
2. Melakukan operasi perkalian dengan nB pada bagian kiri dan kurangkan dari bagian sebelah kanan untuk mendapatkan Pm

   $$\{Pm + kPb\} - nBkG = Pm$$

   dengan,

   $$Pb = nBG$$

   Operasi pengurangan dapat dikonversikan ke penjumlahan dengan mengkalikan -1 pada koordinat y. Operasi ini dibenarkan dengan operasi penjumlahan titik. Pada titik penjumlahan diperoleh refleksi titik melalui $x - axis$.

   Operasi dalam langkah ini menghasilkan Pm yang berbentuk bilangan bulat besar.
3. Mengkonversikan Pm kedalam nilai ASCII

   $\text{IntegerDigits}[\text{big integer}, 65536]$
4. Mengkonversikan hasil dari langkah sebelumnya yang berbentuk nilai ASCII ke karakter yang bersesuaian.

Output :

Teks asli/pesan semula.

Implementasi ECC

Simulasi dilakukan menggunakan Mathematica versi 10.3 di laptop ASUS x2-AP dengan sistem konfigurasi pada intel® @2.16GHz dan 2GB Ram menggunakan 64 bit.

Proses pembentukan kunci :

1. Menentukan bilangan prima p

   $p = 1777$
2. Menentukan nilai a dan b untuk membentuk persamaan kurva eliptik

   $a = -3$

   $b = 101$
3. Menentukan generator G dari pembentukan grup eliptik

   $G = \{\ 12{,}1773\ \}$
4. Membuat kunci privat

   Karena dalam kriptografi kurva eliptik hanya dibutuhkan kunci privat dan kunci publik dari pihak penerima, maka

   $nB = 109$
5. Menghitung kunci publik

   $Pb = nB \cdot G$

   $= \{\ 1364, 986\ \}$

Proses enkripsi :

1. Teks yang dikirim :

   aAbBcCdD 12345)(*&^ UNDIP.
2. Mengkonversi teks kedalam nilai ASCII

   $$\begin{Bmatrix} 97, 65, 98, 66, 99, 67, 100, 68, 32, 49, 50, \\ 51, 52, 53, 32, 41, 40, 42, 38, 94, 32, 85, \\ 78, 68, 73, 80, 46 \end{Bmatrix}$$

   Karena basis yang digunakan 95, maka hasil konversi dikurangkan dengan 32

$$\left\{\begin{matrix}65,33,66,34,67,35,68,36,0,17,18,\\19,20,21,0,9,8,10,6,62,0,53,46,\\36,41,48,14\end{matrix}\right\}$$

3. Menghitung nilai groupsize, yaitu ukuran grup/kelompok yang dipartisi.
   Sebelum menentukan groupsize, terlebih dahulu menghitung konversi bilangan prima p ke basis 95.
   $p = 1777$
   $1777 : 95 = 18\ \boldsymbol{sisa}\ 67$
   $18 : 95 = 0\ \boldsymbol{sisa}\ 18$
   $IntegerDigits[1777,95]$
   $= [18,67]$
   Setelah mendapatkan IntegerDigits, maka mencari group size
   $group\ size$
   $= Length\left[IntegerDigits[p, 65536]\right] - 1$
   $= Length[18,67] - 1$
   $= 2 - 1 = 1$

4. Mempartisi nilai ASCII menjadi beberapa kelompok menurut groupsize.
   Hasil dari group size adalah 1, menyatakan bahwa barisan ASCII tersebut dipartisi dengan setiap grup berisi 1 nilai ASCII. Sehingga hasil partisi sebagai berikut
   $$\left\{\begin{matrix}\{65\},\{33\},\{66\},\{34\},\{67\},\{35\},\{68\},\{36\},\{0\},\\\{17\},\{18\},\{19\},\{20\},\{21\},\{0\},\{9\},\{8\},\{10\},\\\{6\},\{62\},\{0\},\{53\},\{46\},\{36\},\{41\},\{48\},\{14\}\end{matrix}\right\}$$
   Dari perhitungan diatas dapat dilihat bahwa barisan nilai ASCII dari teks menghasilkan 27 grup yang masing-masing berisi 1 nilai ASCII.

5. Mengkonversi setiap grup kedalam ke *big integer*
   $Grup\ 1 = (65 \times 95^0)$
   $= 65$
   Karena setiap grup hanya berisi 1 karakter, maka big integer yang dihasilkan tetap sama dengan nilai sebelumnya.
6. Menambahkan karakter 32 pada akhir data karena grup yang dihasilkan berjumlah ganjil. Namun karena setiap ASCII dikurangi 32, maka penambahan karakter adalah karakter 0. Maka Pm menjadi,
   $$Pm = \left\{\begin{matrix}65,33,66,34,67,35,68,36,0,17,18,\\19,20,21,0,9,8,10,6,62,0,53,46,\\36,41,48,14,0\end{matrix}\right\}$$
   Selanjutnya masing-masing pasangan akan menjadi Pm,
   $Pm_1 = \{65,33\}$
   $Pm_2 = \{66,34\}$
   $Pm_3 = \{67,35\}$
   $Pm_4 = \{68,36\}$
   $Pm_5 = \{0,17\}$
   $Pm_6 = \{18,19\}$
   $Pm_7 = \{20,21\}$
   $Pm_8 = \{0,9\}$
   $Pm_9 = \{8,10\}$
   $Pm_{10} = \{6,62\}$
   $Pm_{11} = \{0,53\}$
   $Pm_{12} = \{46,36\}$
   $Pm_{13} = \{41,48\}$
   $Pm_{14} = \{14,0\}$

7. Memilih nilai k dan menghitung kG dan kPb menggunakan operasi perkalian titik. Perhitungan menggunakan program Mathematica sehingga mendapatkan hasil sebagai berikut
   $k = 337$
   $G = \{12, 1773\}$
   $nB = 109$
   $kG = k \cdot G$
   $= \{1075, 1733\}$
   $Pb = nB \cdot G$
   $= \{1364, 986\}$
   $kPb = k \cdot Pb$
   $= \{1432, 598\}$
8. Menghitung $Pm + kPb$
   $Pm + kPb =$
   $Pm_1 + kPb = \{1362, 1776\}$
   $Pm_2 + kPb = \{430, 245\}$
   $Pm_3 + kPb = \{426, 365\}$
   $Pm_4 + kPb = \{1456, 1117\}$
   $Pm_5 + kPb = \{1131, 327\}$
   $Pm_6 + kPb = \{469, 1185\}$
   $Pm_7 + kPb = \{1734, 736\}$
   $Pm_8 + kPb = \{124, 213\}$
   $Pm_9 + kPb = \{1721, 1454\}$
   $Pm_{10} + kPb = \{199, 982\}$
   $Pm_{11} + kPb = \{1487, 313\}$
   $Pm_{12} + kPb = \{502, 1033\}$
   $Pm_{13} + kPb = \{995, 897\}$
   $Pm_{14} + kPb = \{523, 1559\}$

9. Mengirimkan cipherteks $Pc = \{kG, Pm + kPb\}$ kepada pihak penerima
   $Pc1 = \{\{1075, 1733\}, \{1362, 1776\}\}$
   $Pc2 = \{\{1075, 1733\}, \{430, 245\}\}$
   $Pc3 = \{\{1075, 1733\}, \{426, 365\}\}$
   $Pc4 = \{\{1075, 1733\}, \{1456, 1117\}\}$
   $Pc5 = \{\{1075, 1733\}, \{1131, 327\}\}$
   $Pc6 = \{\{1075, 1733\}, \{469, 1185\}\}$
   $Pc7 = \{\{1075, 1733\}, \{1734, 736\}\}$
   $Pc8 = \{\{1075, 1733\}, \{124, 213\}\}$
   $Pc9 = \{\{1075, 1733\}, \{1721, 1454\}\}$
   $Pc10 = \{\{1075, 1733\}, \{199, 982\}\}$
   $Pc11 = \{\{1075, 1733\}, \{1487, 313\}\}$
   $Pc12 = \{\{1075, 1733\}, \{502, 1033\}\}$
   $Pc13 = \{\{1075, 1733\}, \{995, 897\}\}$
   $Pc14 = \{\{1075, 1733\}, \{523, 1559\}\}$

Proses dekripsi :

1. Mendapatkan cipherteks Pc
   $Pc1 = \{\{1075, 1733\}, \{1362, 1776\}\}$
   $Pc2 = \{\{1075, 1733\}, \{430, 245\}\}$
   $Pc3 = \{\{1075, 1733\}, \{426, 365\}\}$
   $Pc4 = \{\{1075, 1733\}, \{1456, 1117\}\}$
   $Pc5 = \{\{1075, 1733\}, \{1131, 327\}\}$
   $Pc6 = \{\{1075, 1733\}, \{469, 1185\}\}$
   $Pc7 = \{\{1075, 1733\}, \{1734, 736\}\}$
   $Pc8 = \{\{1075, 1733\}, \{124, 213\}\}$
   $Pc9 = \{\{1075, 1733\}, \{1721, 1454\}\}$
   $Pc10 = \{\{1075, 1733\}, \{199, 982\}\}$
   $Pc11 = \{\{1075, 1733\}, \{1487, 313\}\}$
   $Pc12 = \{\{1075, 1733\}, \{502, 1033\}\}$
   $Pc13 = \{\{1075, 1733\}, \{995, 897\}\}$
   $Pc14 = \{\{1075, 1733\}, \{523, 1559\}\}$
2. Memisahkan Pc dengan bagian kiri $\{kG\}$ dan bagian kanan $\{Pm + k\ P\ b\}$

$kG = \{1075, 1733\}$

$Pm_1 + kPb = \{1362, 1776\}$ $Pm_8 + kPb = \{124, 213\}$
$Pm_2 + kPb = \{430, 245\}$ $Pm_9 + kPb = \{1721, 1454\}$
$Pm_3 + kPb = \{426, 365\}$ $Pm_{10} + kPb = \{199, 982\}$
$Pm_4 + kPb = \{1456, 1117\}$ $Pm_{11} + kPb = \{1487, 313\}$
$Pm_5 + kPb = \{1131, 327\}$ $Pm_{12} + kPb = \{502, 1033\}$
$Pm_6 + kPb = \{469, 1185\}$ $Pm_{13} + kPb = \{995, 897\}$
$Pm_7 + kPb = \{1734, 736\}$ $Pm_{14} + kPb = \{523, 1559\}$

3. Melakukan operasi perkalikan dengan nB pada bagian kiri dan kurangkan itu dari bagian sebelah kanan untuk mendapatkan Pm

$$\{Pm + kPb\} - nBkG = Pm$$
$$nBkG = nB \cdot kG$$
$$= \{1432{,}598\}$$

Operasi pengurangan dapat dikonversikan ke penjumlahan dengan mengkalikan -1 pada koordinat y.
$-nBkG = \{1432, -598\}$
Maka Pm yang didapatkan adalah

$Pm_1 = \{65{,}33\}$ $Pm_8 = \{0, 9\}$
$Pm_2 = \{66{,}34\}$ $Pm_9 = \{8, 10\}$
$Pm_3 = \{67{,}35\}$ $Pm_{10} = \{6, 62\}$
$Pm_4 = \{68, 36\}$ $Pm_{11} = \{0, 53\}$
$Pm_5 = \{0, 17\}$ $Pm_{12} = \{46, 36\}$
$Pm_6 = \{18, 19\}$ $Pm_{13} = \{41, 48\}$
$Pm_7 = \{20{,}21\}$ $Pm_{14} = \{14, 0\}$

4. Pm dikonversikan kedalam basis 95

$$Pm = \begin{Bmatrix} 65, 33, 66, 34, 67, 35, 68, 36, 0, 17, 18, \\ 19, 20, 21, 0, 9, 8, 10, 6, 62, 0, 53, 46, \\ 36, 41, 48, 14 \end{Bmatrix}$$

5. Mengkonversikan hasil dari langkah sebelumnya yang berbentuk nilai ASCII ke karakter yang bersesuaian.
   Nilai ASCII :

$$Pm = \begin{Bmatrix} 65, 33, 66, 34, 67, 35, 68, 36, 0, 17, 18, \\ 19, 20, 21, 0, 9, 8, 10, 6, 62, 0, 53, 46, \\ 36, 41, 48, 14, 0 \end{Bmatrix}$$

   Sehingga karakter yang dihasilkan sebagai berikut :

   aAbBcCdD 12345)(*&^ UNDIP.

D. PENUTUP

Simpulan

Dari pembahasan yang telah dilakukan, dapat diambil kesimpulan bahwa proses kriptografi dengan kurva eliptik itu dimulai dari proses pembentukan kunci. Generator G adalah pembangkit kunci yang digunakan untuk menghitung kunci publik. Generator G didapatkan dari grup eliptik yaitu himpunan titik-titik kurva eliptik atas $GF(p)$. Setelah membentuk kunci privat dan kunci publik, kemudian melakukan proses enkripsi. Proses enkripsi disini berproses 2 kali, mengubah pesan asli menjadi plainteks dan mengubah plainteks menjadi cipherteks. Pesan asli akan dirubah menjadi plainteks yang berbentuk sebuah titik, yang mana titik tersebut yang akan dilakukan algoritma enkripsi menjadi cipherteks. Cipherteks yang didapatkan oleh penerima akan didekripsi menggunakan algoritma dekripsi kriptografi kurva eliptik dengan bantuan kunci privat. Semakin besar p yang digunakan, maka banyak grup yang dihasilkan akan semakin banyak. Sehingga titik cipherteks yang dihasilkan juga semakin banyak.

Peran aljabar untuk lapangan Galois prima adalah sebagai dasar dari pembentukan kunci dan perhitungan dalam algoritma enkripsi maupun dekripsi. Perhitungan menggunakan modulo p, yang mana bilangan prima adalah dasar dari pembentukan kriptografi kurva eliptik tersebut. Kunci terbentuk dari sebuah persamaan kurva eliptik yang terdefinisi atas modular prima. Perhitungan yang berulang kali dalam pembentukan kunci juga membutuhkan dasar grup siklik.

Saran

Saran dari pembahasan ini adalah perlunya dikembangkan lagi mengenai kriptografi kurva eliptik dengan basis yang berbeda dan kriptografi kurva eliptik biner.

E. DAFTAR PUSTAKA

Certicom. 2000. *SEC1: Elliptic Curve Elliptic*. Certicom corp.

Harkenson, Darel. 2004. *Guide to Elliptic Curve Cryptography*. USA : Springer-Verlag New York, Inc.

Lidl, Rudolf. 1994. *Introduction to Finite Fields and Their Applications*. Australia : Cambridge University Press.

Menezes, Oorcshot, and Vanstone. 1996. *Handbook of Applied Cryptography*, USA : CRC Press, Inc

Sadikin, Rifki. 2012. *Kriptografi untuk keamanan jaringan*. Yogyakarta : Andi.

Singh, Laiphrakpam Dolendro., Singh, Khumanthem Manglem., 2015. Implementation of Text Encryption using Elliptic Curve Cryptography. *Procedia Computer Science*, Vol 73, hlm 73-82.

Stefen, Dr. Andreas. 2002. *The Elliptic Curve Cryptosystem*. Zürcher Hochschule Winterthur

Wahyu, Puguh dan Zaki Riyanto. 2010. *Penerapan Kurva Eliptik Atas Zp Pada Skema Tanda Tangan Elgamal*. Paper. Jogja : Universitas Gajah mada.