JOURNAL OF FUNDAMENTAL MATHEMATICS
AND APPLICATIONS (JFMA) VOL. 4 NO. 1 (JUN 2021)
Available online at www.jfma.math.fsm.undip.ac.id

IMPLEMENTASI KRIPTOGRAFI KURVA ELIPTIK ELGAMAL DI LAPANGAN GALOIS PRIMA PADA PROSES ENKRIPSI DAN DEKRIPSI BERBANTUAN *SOFTWARE PYTHON*

Ummu Wachidatul Latifah[1], Puguh Wahyu Prasetyo[2]

[1]*Departemen Matematika, Fakultas Sains dan Teknologi Terapan, Universitas Ahmad Dahlan Yogyakarta*
[2]*Departemen Pendidikan Matematika, Fakultas Keguruan dan Ilmu Pendidikan, Universitas Ahmad Dahlan Yogyakarta*
Email: [1]ummu1600015054@webmail.uad.ac.id, [2]puguh.prasetyo@pmat.uad.ac.id

Abstract. The development of technology has an impact on the progress in all areas of human life, especially in the field of information. The development of technology also has positive and negative implications. One of the positive effects is the ease of exchanging information from the public or confidential over the internet. The negative impact is that personal data becomes less secure and can be misused by unauthorized parties. Elliptic Curve Cryptography (ECC) provides a solution for the security of information. ECC is one of the public key cryptography with a high level of protection compared to other public-key algorithms. This research aims to understand the cryptographic concept of the elliptic curve ElGamal process that will be defined in the prime Galois field. This study uses ElGamal elliptic curves in the Galois field for key formation processes, encryption processes, and decryption processes in data using Python.
Keywords: Cryptography, Elliptic Curve ElGamal, Prime Galois Field, Python

Abstrak. Perkembangan teknologi memberikan dampak terhadap kemajuan di segala bidang kehidupan manusia terutama dalam bidang informasi. Hal ini memberikan dampak positif dan negatif. Salah satu dampak positifnya adalah mudahnya bertukar informasi dari yang bersifat umum atau rahasia melalui internet. Dampak negatifnya adalah data yang bersifat rahasia menjadi kurang aman dan dapat disalahgunakan oleh pihak yang tidak berwenang. Kriptografi kurva eliptik ElGamal (*ECC: Eliptic Curve Cryptosystem*) memberikan solusi untuk keamanan suatu informasi. *ECC* merupakan salah satu metode kriptografi kunci publik yang mempunyai tingkat keamanan tinggi dibandingkan dengan algoritma kunci publik lainnya. Tujuan dari penelitian ini adalah memahami konsep kriptografi kurva eliptik ElGamal yang akan didefinisikan di Galois *field* prima. Hasil dari penelitian ini, yaitu penggunaan kurva eliptik ElGamal di Galois *field* prima untuk proses pembentukan kunci, proses enkripsi dan proses dekripsi pada suatu data dengan menggunakan *Python.*
Kata Kunci: kriptografi, kurva eliptik ElGamal, Lapangan Galois prima, *Python*

I. PENDAHULUAN

Perkembangan teknologi dan informasi saat ini sangatlah pesat. Hal tersebut dapat mempercepat dan mempermudah pertukaran informasi atau data. Namun kemudahan tersebut

menjadi salah satu masalah yang dihadapi dalam pemanfaatan teknologi dan informasi, karena mudahnya terjadi pencurian informasi atau data rahasia oleh pihak yang tidak berwenang. Untuk menghindari hal tesebut, maka diperlukan suatu sistem keamanan yang dapat mengamankan informasi atau data. Salah satu ilmu yang mempelajari sistem keamanan, yaitu kriptografi.

Kriptografi merupakan ilmu dan seni untuk menyembunyikan pesan. Berdasarkan kuncinya, algoritma kriptografi terbagi menjadi dua, yaitu algoritma simetris (algoritma kunci privat) dan algoritma asimetris (algoritma kunci publik). Kriptografi simetris, yaitu algoritma kriptografi yang hanya menggunakan satu buah kunci untuk proses enkripsi dan dekripsi. Proses enkripsi, yaitu proses menyandikan pesan asli (*plaintext*) menjadi pesan yang sulit dibaca (*ciphertext*) dan proses dekripsi, yaitu proses pengembalian pesan yang sulit dibaca (*ciphertext*) menjadi pesan asli (*plaintext*). Contoh algoritma kriptografi simetris, yaitu DES (*Data Encryption Standard*) dan AES (*Advanced Encryption Standard*). Kriptografi asimetris, yaitu algoritma kriptografi yang menggunakan dua buah kunci untuk proses enkripsi dan proses dekripsi. Contoh algoritma kriptografi asimetris, yaitu kriptografi kurva eliptik dan RSA.

Kriptografi kurva eliptik merupakan kriptografi kunci publik yang membutuhkan komputasi tinggi karena perhitungan algoritma yang kompleks. Namun di sisi lain hal tersebut memberikan keuntungan, yaitu semakin kompleks perhitungan semakin sulit untuk dipecahkan atau semakin tinggi tingkat keamanannya. Salah satu solusi yang ditawarkan adalah menerapkan perhitungan aritmetika di lapangan komposit (*composit field*) [1].

Kriptografi kurva eliptik ditemukan oleh Koblitz dan Miller pada tahun 1986. Kriptografi kurva eliptik menjadi pilihan alternatif yang sering digunakan karena mempunyai tingkat keamanan lebih tinggi dengan panjang kunci yang pendek dibandingkan dengan algoritma RSA [2].

Dalam kriptografi kunci publik, lapangan hingga atau Galois *field* maupun grup Galois memegang peranan yang sangat penting. Beberapa implementasi grup Galois dapat ditemukan dalam [3] dan [4]. Lebih lanjut, ada beberapa algoritma kunci publik yang mendefinisikan perhitungan aritmetika di lapangan berhingga atau Galois *field*, salah satunya kriptografi kurva eliptik El Gamal. Implementasi El Gamal dalam dalam proses enkripsi warna pada gambar seperti ditunjukkan oleh hasil penelitian dalam [5] dan [6]. Selain itu juga digunakan dalam proses identifikasi keaslian pesan atau disebut juga dengan istilah autentifikasi [7].

Semua perhitungan kriptografi kurva eliptik didefinisikan di Galois *field* prima atau GF_p yang penerapannya analog dengan kriptosistem ElGamal. Untuk mempermudah perhitungan aritmetika yang sulit di Galois *field* tersebut diperlukan adanya sebuah *software*. *Software* yang akan digunakan dalam proses penelitian ini, yaitu *Python*.

Python merupakan pemrograman interpretatif multiguna dengan filosofi perancangan yang berfokus pada tingkat keterbacaan kode. *Python* diklaim sebagai bahasa yang menggabungkan kapabilitas, kemampuan, dengan sintaksis kode yang sangat jelas, dan dilengkapi dengan fungsionalitas pustaka standar yang besar serta komprehensif [8].

Dalam penelitian ini akan dibahas implementasi kriptografi kurva eliptik ElGamal dalam proses enkripsi dan dekripsi pada Galois *field* prima menggunakan *Python*.

II. KONSEP DASAR KRIPTOGRAFI KURVA ELIPTIK EL GAMAL

2.1 Kriptografi Kurva Eliptik

Kriptografi kurva eliptik merupakan salah satu sistem kriptografi kunci publik yang mendasarkan keamanannya pada masalah kurva elips. Penentuan titik-titik kurva eliptik merupakan masalah logaritma diskrit yang sulit diselesaikan. Oleh karena itu algoritma kriptografi kurva eliptik ini memiliki keunggulan dibandingkan dengan algoritma kriptografi kunci public yang lainnya, yaitu memiliki tingkat keamanan yang sama dengan ukuran kunci yang lebih pendek [9].

Ada tiga protokol kurva eliptik yang diketahui, yaitu ECDSA (*Elliptic Curve Digital Signature),* ECDH (*Elliptic Curve Diffie-Helman)* dan EC ElGamal (*Elliptic Curve El Gamal).* Pada bagian ini ini akan dibahas mengenai konsep EC ElGamal.

Konsep yang mendasari penentuan titik-titik pada kurva elitpik, yaitu grafik atau kurva yang dibentuk dari persamaan:

$$y^2 = x^3 + ax + b \tag{2}$$

dengan a, b merupakan konstanta. Persamaan tersebut sering disebut sebagai persamaan Weierstrass yang didefinisikan pada lapangan hingga. Secara umum, bentuk persamaan Weierstrass sebagai berikut:

$$y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6 \tag{3}$$

dengan $a_1, a_2, \ldots, a_6$ merupakan konstanta. Apabila persamaan (2) didefinisikan pada lapangan yang memiliki karakteristik k dengan $k \neq 2$ maka diperoleh:

$$\left(y + \frac{a_1x}{2} + \frac{a_3}{2}\right)^2 = x^3 + \left(a_2 + \frac{a_1^2}{4}\right)x^2 + \left(a_4 + \frac{a_1a_3}{4}\right)x + \left(\frac{a_3^2}{4} + a_6\right) \tag{4}$$

Persamaan (3) dapat ditulis menjadi:

$$y_1^2 = x^3 + a_2'x^2 + a_4'x + a_6 \tag{5}$$

dengan $y_1 = y + \frac{a_1x}{2} + \frac{a_3}{2}$ dan a_2', a_4' dan a_6' merupakan konstanta. Jika karakterikstik lapangan tidak sama dengan 3, maka dari persamaan (5) diperoleh:

$$y_1^2 = x_1^3 + ax_1 + b \tag{6}$$

dengan $x_1 = x + \frac{a_2'}{3}$ dan a, b merupakan suatu konstanta. Persamaan (6) identik dengan persamaan (2), yaitu $y_2 = x^3 + ax + b$. Persamaan (2) disebut dengan *depressed cubic equation.* Solusi persamaan tersebut telah ditemukan oleh Girolamo Cardano. Berikut bentuk solusinya:

$$x = \sqrt[3]{-\frac{b}{2} + \sqrt{\frac{b^2}{4} + \frac{a^3}{27}}} + \sqrt[3]{-\frac{b}{2} - \sqrt{\frac{b^2}{4} + \frac{a^3}{27}}} \tag{7}$$

dari persamaan (7) diperoleh diskriminan dari persamaan (2), yaitu:

$$D = 4a^3 + 27b^2 \neq 0. \quad (8)$$

Terdapat dua jenis kurva eliptik yang utama, yaitu: kurva eliptik yang mempunyai tiga nyata berbeda dan kurva eliptik yang mempunyai akar tunggal. Kurva eliptik yang akan digunakan dalam penelitian ini tidak boleh mempunyai akar kembar. Dengan kata lain, suatu kurva eliptik mempunyai akar kembar jika $4a^3 + 27b^2 = 0$ [10].

2.2 Kurva Eliptik di GF_p

Kriptografi kurva eliptik yang didefinisikan dengan menggunakan daerah karakteristik bilangan prima atau GF_p, dimana p merupakan bilangan prima yang lebih besar dari 3. Sebuah kurva eliptik E pada GF_p didefinisikan dalam persamaan sebagai berikut:

$$y^2 = x^3 + ax + b \quad (9)$$

dimana $a, b \in GF_p$ dan $4a^3 + 27b^2 \ (mod\ p) \neq 0$ dan sebuah titik (O) yang disebut titik tak hingga (*infinity*). Titik tak hingga merupakan identitas. Himpunan $E(\ GF_p\ )$ merupakan semua titik (x, y) untuk $x, y \in GF_p$ yang memenuhi persamaan (8) pada titik (O) [11].

Proses enkripsi dan dekripsi dalam kurva eliptik pada GF_p menggunakan operasi aljabar, yaitu penjumlahan, pengurangan dan penggandaan titik [12]. Perhitungan dapat dilakukan sebagai berikut:

1. Penjumlahan Titik
   Misal diketahui $M(\ x_1\ , y_1\ )$ dan $(\ x_1\ , y_2\ )$, dimana $M \neq N\ , M + N = R$. Untuk mencari koordinat , diperlukan x_3 dan y_3 . Titik x_3 dapat diperoleh dengan menggunakan persamaan (10) dan titik y_3 dapat diperoleh dengan menggunakan persamaan (11) sebagai berikut:
   $$x_3 = (\lambda^2 - x_1 - x_2)\ mod\ p \quad (10)$$
   $$y_3 = (\lambda(x_1 - x_3) - y_1) mod\ p \quad (11)$$
   dengan $\lambda = \frac{y_2 - y_1}{x_2 - x_1} mod\ p$

2. Pengurangan titik
   Operasi pengurangan dapat dilakukan dengan menjumlahkan satu titik dengan nilai negatif dari titik lainnya. Misalkan $P(x_p\ , y_p)$ dan $Q(x_q\ , y_q)$. Pengurangan:
   $$P - Q = P + (-Q), \quad (12)$$
   yang dalam hal ini $-Q = (x_q, -\ y_q\ (mod\ p))$.

3. Penggandaan titik
   Misalkan diketahui titik $M(x_1, y_1)$ dan (x_1, y_2), dengan $M = N$, maka untuk menggandakan titik x dapat menggunakan persamaan (13) dan untuk menggandakan titik y dapat menggunakan persamaan (14).

$$x_3 = (\lambda^2 - 2x_1)\ mod\ p \tag{13}$$

$$y_3 = (\lambda(x_1 - x_3) - y_1) mod\ p \tag{14}$$

dengan $\lambda = \frac{3x_1^2 + a}{2y_1} mod\ p$.

2.3 Algoritma Pembentukan Kunci Kriptografi Kurva Eliptik

Kriptografi kurva eliptik merupakan salah satu kriptografi asimetris, yaitu kriptografi yang mempunyai dua kunci. Kunci publik dan kunci privat. Kunci publik merupakan kunci yang digunakan untuk enkripsi. Sedangkan kunci untuk dekripsi menggunakan kunci rahasia [13].

Berikut merupakan langkah-langkah yang dilakukan dalam pembuatan kunci kriptografi kurva eliptik:[9]

1. Menentukan bilangan prima p, dengan syarat $p > 3$.
2. Menentukan persamaan kurva eliptik yang memenuhi syarat $4a^3 + 27b^2\ (mod\ p)\ \neq\ 0$
3. Mencari sisa kuadratik QR_p
4. Menentukan titik generator G, dari grup eliptik atas GF_p
5. Menentukan kunci privat d. Kunci privat d ditentukan dengan nilai acak dimana nilai kunci tersebut merupakan elemen dari $d \in 2,3, \dots, p-1$ dalam F_p.
6. Menghitung kunci publik Q. Kunci publik $Q = d \cdot G$. Kunci publik dihitung oleh masing-masing pengguna dengan melakukan operasi perkalian titik antara kunci rahasia masing-masing dengan titik G.

2.4 Kriptografi Kurva Eliptik El Gamal

Kriptografi kurva eliptik ElGamal atau yang sering dikenal dengan *Elliptic Curve Cryptosystem* merupakan sebuah kriptosistem dengan menggunakan kunci yang telah dibangkitkan dari titik-titik kurva eliptik. Untuk proses selanjutnya, yaitu proses enkripsi dan dekripsi.

2.4.1 Proses Enkripsi

Proses enkripsi merupakan proses mengubah pesan asli (*plaintext*) menjadi pesan rahasia (*ciphertext*). Adapun langkah-langkah yang dilakukan dalam proses enkripsi adalah sebagai berikut [11], [14]:

Algoritma Enkripsi

Input: Parameter p, G, E, n, kunci publik Q, pesan asli M.
Output: *Ciphertext* (C_1 , C_2)

1. Mengonversi pesan asli menjadi titik-titik kurva eliptik yang telah ditentukan.
2. Memilih suatu bilangan acak $k \in [\, 1, n-1\,]$
3. Menghitung nilai $(C_1\,, C_2)$ yang merupakan *ciphertext*, dengan $C_1 = k.G$
4. Menghitung nilai C_2 menggunakan rumus $C_2 = M + k.Q$ dimana M merupakan *plaintext* yang sudah dikonversikan ke dalam titik-titik kurva eliptik dan Q merupakan kunci publik.
5. Diperoleh *ciphertext* (C_1, C_2)

Gambar 1. Algoritma enkripsi yang digunakan

2.4.2 Proses Dekripsi

Proses dekripsi merupakan proses mengubah pesan rahasia (*ciphertext*) menjadi pesan asli (*plaintext*). Adapun langkah-langkah yang dilakukan saat proses dekripsi, yaitu:

Algoritma Dekripsi

Input: Parameter p, G, E, n, kunci privat d, *Ciphertex*t (C_1, C_2).
Output: Pesan asli (M)

1. Hitung $M = C_2 - d.C_1$
2. Hasil M

Gambar 2. Algoritma dekripsi yang digunakan

III. METODE PENELITIAN

Penelitian ini dilakukan berdasarkan kajian pustaka, pengembangan model kriptografi kurva eliptik dan implementasi model ke dalam program komputer dengan rincian sebagai berikut:

3.1 Tahap Awal Penelitian

Berdasarkan data yang diperoleh dari berbagai sumber seperti jurnal ilmiah, buku, ataupun penelitian sebelumnya, maka diperoleh beberapa metode analisis yang dilakukan dalam penelitian ini:

1. Mengumpulkan data berupa teori mengenai kriptografi kurva eliptik ElGamal.
2. Menentukan nilai a, b dan p untuk dapat memperoleh persamaan kurva eliptik pada lapangan Galois *field* (GF_p).

3. Menentukan elemen-elemen grup eliptik $E(GF_p)$ dengan cara menghitung nilai residu kuadrat modulo p kemudian membandingkannya dengan nilai dari persamaan $y^2 = x^3 + ax + b \ (mod\ p)$.
4. Menentukan grup P sebagai generator dari grup eliptik (GF_p).
5. Menentukan domain kurva eliptik.
6. Mencari algoritma kriptografi kurva eliptik pada skema enkripsi ElGamal.
7. Merepresentasikan titik-titik kurva eliptik dengan simbol yang dipilih.
8. Menentukan kunci yang akan digunakan.
9. Melakukan enkripsi pesan yang akan diamankan.
10. Melakukan proses dekripsi pesan.

3.2 Proses Konstruksi

Program yang akan dibuat memiliki tampilan awal (menu utama) yang memiliki beberapa pilihan, yaitu pembentukan titik-titik kurva eliptik, pembentukan kunci, enkripsi dan dekripsi. Hasil pembentukan kunci kemudian disimpan menjadi dua buah file objek *Python* yang masing-masing berisi kunci publik dan kunci rahasia. Input dari proses enkripsi berupa *plaintext* yang akan dienkripsi dengan output berupa *ciphertext* disimpan ke dalam sebuah file objek *Python*. Sementara dalam proses dekripsi, input berupa file objek *Python* yang berisi *ciphertext* dan file objek *Python* kunci rahasia dengan output berupa *plaintext* hasil dekripsi.

3.3 Proses Pengujian

Pada tahap ini dilakukan pengujian terhadap *output* program yang diperoleh. Pengujian berupa pengecekan hasil *plaintext* yang sudah mengalami proses enkripsi dan dekripsi apakah sama dengan *plaintext* aslinya atau tidak.

IV. HASIL DAN DISKUSI

4.1 Pembentukan Titik-titik Kurva Eliptik di GF_p

Langkah pertama dalam kriptografi kurva eliptik, yaitu menentukan titik-titik kurva eliptik. Misalkan dipilih nilai $p = 13$. Kemudian menentukan nilai a, b yang merupakan bilangan bulat positif. Dipilih nilai $a = 4$ dan $b = 7$. Menentukan persamaan kurva eliptik dengan nilai $a = 4, b = 7$ dan $p = 13$, sehingga diperoleh:

$$y^2 = x^3 + 4x + 7 \ (mod\ 13)$$

Diperiksa jika a, b dan p memenuhi persamaan $4a^3 + 27b^2 (mod\ p) \neq 0$ maka persamaan kurva eliptik tersebut dapat berlaku.

$4a^3 + 27b^2 (mod\ p) \neq 0$
$4.4^3 + 27.7^2 (mod\ 13) \neq 0$
$4.4^3 + 27.7^2 (mod\ 13) = 4096 + 1323 \ (mod\ 13)$
$4.4^3 + 27.7^2 (mod\ 13) = 5419 \ (mod\ 13) = 8 \neq 0$

Maka diperoleh persamaan kurva eliptik:

$$y^2 = x^3 + 4x + 7 \ (mod\ 13)$$

Untuk dapat membuat titik (x, y) maka tentukan terlebih dahulu elemen dari kurva eliptik $E_{13}(4,7)$ atas GF_{13}, sebagai berikut: $GF_{13} = \{0,1,2,3,4,5,6,7,8,9,10,11,12\}$. Sebelum membentuk semua titik (x, y) tenukan terlebih dahulu daerah elemen/ *range* kurva eliptik QR_{13} (*Quadratic Residue Module*). Pada Tabel 1 berikut ini merupakan *quadratic residue module* dari GF_{13}

Tabel 1 *Quadratic Residue Modulo* 13

GF_p	$y^2\ (mod\ 13)$	QR_{13}
0	$0^2 (mod\ 13)$	0
1	$1^2 (mod\ 13)$	1
2	$2^2 (mod\ 13)$	4
3	$3^2 (mod\ 13)$	9
4	$4^2 (mod\ 13)$	3
5	$5^2 (mod\ 13)$	12
6	$6^2 (mod\ 13)$	10
7	$7^2 (mod\ 13)$	10
8	$8^2 (mod\ 13)$	12
9	$9^2 (mod\ 13)$	3
10	$10^2 (mod\ 13)$	9
11	$11^2 (mod\ 13)$	4
12	$12^2 (mod\ 13)$	1

Dari Tabel 1 di atas, diperoleh $QR_{13} = \{0,1,3,4,9,10,12\}$. Selanjutnya, akan ditentukan elemen grup kurva eliptik $E_{13}(4,7)$ yang merupakan himpunan penyelesaian dari $y^2 = x^3 + 4x + 7\ (mod\ 13)$ untuk $x \in GF_{13}$ dan $y^2 \in QR_{13}$. Berikut ini dalam Tabel 2 diberikan elemen-elemen dari gurp kurva eliptik yang terbentuk dari kurva eliptik $y^2 = x^3 + 4x + 7$ atas lapangan Galois prima GF_{13}.

Tabel 2. Elemen Grup Kurva Eliptik yang dibentuk dari $y^2 = x^3 + 4x + 7\ (mod\ 13)$ atas GF_{13}

x	$y^2 = x^3 + 4x + 7\ (mod\ 13)$	$y^2 \in QR_{13}$	$(x, y) \in E_{13}(4,7)$
0	$y^2 = 0^3 + 4.0 + 7\ (mod\ 13) = 7$	$y^2 \notin QR_{13}$	–
1	$y^2 = 1^3 + 4.1 + 7\ (mod\ 13) = 12$	$y^2 \in QR_{13}$	(1,5) & (1,8)
2	$y^2 = 2^3 + 4.2 + 7\ (mod\ 13) = 10$	$y^2 \in QR_{13}$	(2,6) & (2,7)
3	$y^2 = 3^3 + 4.3 + 7\ (mod\ 13) = 7$	$y^2 \notin QR_{13}$	–
4	$y^2 = 4^3 + 4.4 + 7\ (mod\ 13) = 9$	$y^2 \in QR_{13}$	(4,3) & (4,10)
5	$y^2 = 5^3 + 4.5 + 7\ (mod\ 13) = 9$	$y^2 \in QR_{13}$	(5,3) & (5,10)
6	$y^2 = 6^3 + 4.6 + 7\ (mod\ 13) = 0$	$y^2 \in QR_{13}$	(6,0)
7	$y^2 = 7^3 + 4.7 + 7\ (mod\ 13) = 1$	$y^2 \in QR_{13}$	(7,1) & (7,12)
8	$y^2 = 8^3 + 4.8 + 7\ (mod\ 13) = 5$	$y^2 \notin QR_{13}$	–
9	$y^2 = 9^3 + 4.9 + 7\ (mod\ 13) = 5$	$y^2 \notin QR_{13}$	–

10	$y^2 = 10^3 + 4.10 + 7 \ (mod\ 13) = 7$	$y^2 \notin QR_{13}$	−
11	$y^2 = 11^3 + 4.11 + 7 \ (mod\ 13) = 4$	$y^2 \in QR_{13}$	$(11,2)$ & $(11,11)$
12	$y^2 = 12^3 + 4.12 + 7 \ (mod\ 13) = 2$	$y^2 \notin QR_{13}$	−

Oleh sebab itu diperoleh Grup Eliptik sebagai berikut:
$E_{13}(4,7) = \{(1,5), (1,8), (2,6), (2,7), (4,3), (4,10), (5,3), (5,10), (6,0), (7,1), (7,12), (11,2), (11,11)\}$.
Setelah itu memilih salah satu titik yang akan dijadikan generator atau pembangkit G. Untuk merepresentasikan titik-titik kurva eliptik terhadap simbol bilangan, huruf dan yang lainnya dilakukan dengan menentukan pembangkit, yaitu G. Representasi tersebut tergantung dengan titik yang dipilih, sehingga hal tersebut tidak dapat berlaku secara umum.

4.2 Pembentukan Kunci Kurva Eliptik

Kekuatan dari kriptografi ini adalah banyaknya titik yang terdapat pada sebuah kurva dan sulit untuk mengetahui bentuk kurva seperti apa yang digunakan. Kriptografi kurva eliptik menggunakan dua kunci untuk proses enkripsi dan dekripsi. Kunci publik dan kunci privat. Kunci publik, yaitu titik pada kurva bersifat acak yang diperoleh dari perkalian antara kunci privat dengan titik pembangkit atau generator G dan kunci privat adalah angka yang kita tentukan sendiri. Berikut ini akan diberikan contoh pembentukan kunci publik dan kunci privat.

Pada pembahasan **4.1** diambil contoh $a = 4, b = 7$ dan $p = 13$. Dari nilai a, b dan p diperoleh suatu grup kurva eliptik, yaitu
$E_{13}(4,7) = \{(1,5), (1,8), (2,6), (2,7), (4,3), (4,10), (5,3), (5,10), (6,0), (7,1), (7,12), (11,2), (11,11)\}$.
Langkah selanjutnya, yaitu menentukan titik pembangkit atau generator $G \in E_{13}(4,7)$. Sebagai contoh diambil $G = (2,6)$. Selanjutnya menentukan kunci privat d. Kunci privat ditentukan secara acak dengan syarat $d \in 2,3, \ldots p - 1 \in GF_p$. Sebagai contoh akan ditentukan $d = 3$.

Setelah menentukan generator $G = (2,6)$ dan kunci privat $d = 3$, maka langkah selanjutnya yaitu menghitung kunci publik Q dengan menggunakan persamaan penjumlahan titik kurva eliptik pada GF_p antara nilai d dan titik G.

$$\begin{aligned} Q &= d.G \\ &= 3.(2,6) \\ &= (2,6) + (2,6) + (2,6) \\ &= (5,3) + (2,6) \\ &= (7,12) \end{aligned}$$

diperoleh nilai kunci publik $Q = (7,12)$.

4.3 Kriptografi Kurva Eliptik ElGamal

Kriptografi kurva eliptik El Gamal merupakan salah satu kriptografi yang sistemnya analog atau sesuai dengan protokol kurva eliptik. Pada sistem kriptografi kurva eliptik El Gamal terdapat proses enkripsi dan dekripsi.

4.3.1 Proses Enkripsi

Berdasarkan pembahasan **4.1** dan **4.2** dengan nilai $a = 4, b = 7$ dan $p = 13$ diperoleh titik-titik kurva eliptik, nilai kunci privat dan kunci publik. Untuk melakukan enkripsi pada suatu pesan, maka perlu dilakukan langkah-langkah algoritma enkripsi. Akan diambil contoh huruf AB, berikut langkah-langkah enkripsi kriptografi kurva eliptik:

1. Langkah awal proses enkripsi, yaitu menentukan titik pembangkit yang dalam penelitian ini memilih contoh $G = (2,6)$ sebagai representasi huruf A. Huruf A dapat dituliskan sebagai θ, maka diperoleh $A = \theta = (2,6)$. Sedangkan huruf B dapat dituliskan sebagai 2θ, sehingga diperoleh $B = 2\theta = (5,3)$. Nilai 2θ dapat dicari dengan menggunakan operasi penggandaan titik-titik kurva eliptik. Untuk huruf, angka dan symbol yang lainnya dapat direpresentasikan menjadi $3\theta, 4\theta, \dots n\theta$ dengan menggunakan operasi penjumlahan atau penggandaan titik kurva eliptik.
2. Langkah selanjutnya, yaitu memilih suatu bilangan acak $k \in [\,1, n-1\,]$. Dipilih $k = 4$.
3. Menghitung nilai $(C_1\,, C_2)$ yang merupakan *ciphertext*, dengan $C_1 = k.G$. karena nilai C_1 sama untuk setiap representasi symbol menjadi titik –titik kurva eliptik, maka cukup dihitung satu kali. Diketahui nilai $k = 4$ dan nilai $G = (2,6)$, maka dengan menggunakan operasi penjumlahan dan penggandaan titik-tiitk kurva eliptik diperoleh:
   $C_1 = k.G$
   $= 5.(2,6)$
   $= (2,6) + (2,6) + (2,6) + (2,6) + (2,6)$
   $= (5,3) + (5,3) + (2,6)$
   $= (5,10)$
4. Menghitung nilai C_2 menggunakan rumus $C_2 = M + k.Q$. M merupakan *plaintext* yang sudah dikonversikan ke dalam titik-titik kurva eliptik, $Q = (7,12)$ merupakan kunci publik dan $k = 5$ dengan menggunakan operasi penggandaan dan penjumlahan titik-titik kurva eliptik.
   Untuk C_2 A, diperoleh:
   $C_2 = M + k.Q$
   $= (2,6) + 5.(7,12)$
   $= (2,6) + \big((7,12) + (7,12) + (7,12) + (7,12) + (7,12)\big)$
   $= (2,6) + \big((2,7) + (2,7) + (7,12)\big)$
   $= (2,6) + \big((5,10) + (7,12)\big)$
   $= (5,3)$
   Untuk C_2 B, diperoleh:
   $C_2 = M + k.Q$
   $= (5,3) + 5.(7,12)$
   $= (5,3) + \big((7,12) + (7,12) + (7,12) + (7,12) + (7,12)\big)$
   $= (5,3) + \big((2,7) + (2,7) + (7,12)\big)$
   $= (5,3) + \big((5,10) + (7,12)\big)$
   $= (7,12)$
5. Diperoleh *ciphertext* untuk huruf $A = (C_1, C_2) = \big((5,10),(5,3)\big)$ dan *ciphertext* untuk huruf $B = (C_1, C_2) = \big((5,10),(7,12)\big)$.

4.3.2 Proses Dekripsi

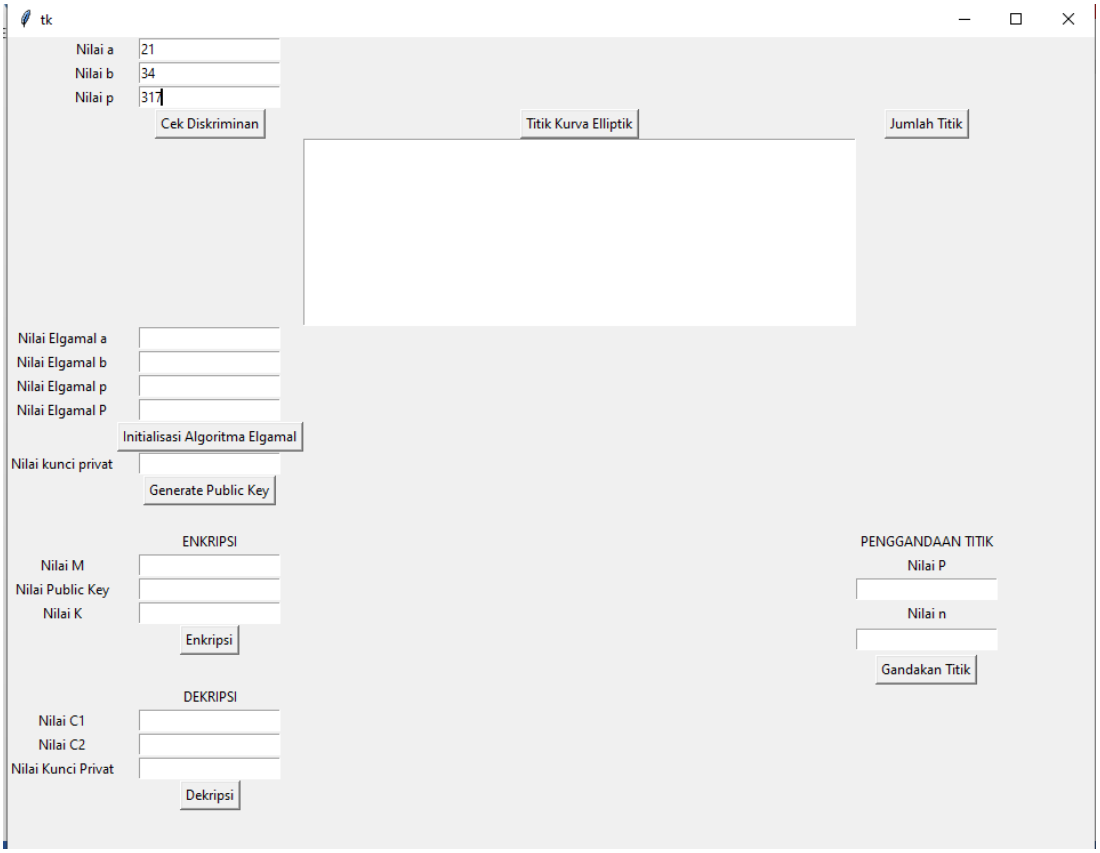
Berdasarkan **4.3.1** diperoleh bahwa nilai *ciphertext* dari $B = \big((5{,}10),(5{,}3)\big)$ $\big((5{,}10),(7{,}12)\big)$. Supaya pesan dapat terbaca, maka perlu dilakukan proses dekripsi. Berikut langkah-langkah dekripsi pesan:

1. Menghitung nilai pesan teks $M = C_2 - d.C_1$, dengan kunci privat $d = 3$.
   $M = (5{,}3) - 3.(5{,}10)$
   $= (5{,}3) - \big((5{,}10) + (5{,}10) + (5{,}10)\big)$
   $= (5{,}3) - \big((7{,}12) + (5{,}10)\big)$
   $= (2{,}6) = A$
   $M = (7{,}12) - 3.(5{,}10)$
   $= (7{,}12) - \big((5{,}10) + (5{,}10) + (5{,}10)\big)$
   $= (7{,}12) - \big((7{,}12) + (5{,}10)\big)$
   $= (5{,}3) = B$
2. Hasil M
   Diperoleh pesan asli, yaitu AB

4.4 Implementasi pada *Phyton*

Proses penghitungan titik-titik kurva eliptik, proses enkripsi dan proses dekripsi pada kriptografi kurva eliptik El Gamal merupakan perhitungan matematika yang sulit dan memerlukan banyak waktu, sehingga akan sangat terbatas nilainya apabila dilakukan secara manual. Oleh karena itu, penulis mencoba mengimplementasikan algoritma kriptografi kurva eliptik El Gamal di Galois $field$ prima dengan menggunakan *software Python,* yaitu berbentuk *GUI.* Adanya *GUI Python* diharapkan dapat meningkatkan keamanan sistem dengan menggunakan nilai yang lebih besar dan mpercepat proses penentuan titik-titik kurva eliptik, proses enkripsi dan proses dekripsi pada algoritma kriptografi El Gamal.

Diambil contoh nilai $a = 21, b = 34$ dan $p = 317$. Berikut tampilan awal *GUI Python* dapat dilihat pada Gambar 3 di bawah ini:



Gambar 3. Tampilan GUI dengan *Phyton*

4.4.1 Pembentukan Titik-titik Kurva Eliptik

Sebelum melakukan proses enkripsi, maka langkah awal adalah memastikan bahwa diskriminan dari kurva eliptik yang digunakan tidak sama dengan 0. Dalam proses ini, yang digunakan adalah $y^2 = x^3 + 21x + 34$ dengan bilangan prima $p = 317$. Dengan menggunakan program yang telah dikontruksi, maka diperoleh tampilan seperti yang ditunjukkan oleh Gambar 4 di bawah ini.

Gambar 4. Pembentukan titik-titik dalam $y^2 = x^3 + 21x + 34$ atas $p = 317$

4.4.2 Penggandaan Titik

Dengan memilih titik $P = (3,21)$ sebagai pembangkit, maka langkah berikutnya adalah penggandaan titik yang prosesnya dengan program yang telah dikonstruksi dapat dilihat pada Gambar 5 berikut ini.

Gambar 5. Penggandaan Titik $P = (3,21)$

4.4.3 Representasi Titik-titik Kurva Eliptik

Untuk menyederhanakan proses simulasi kriptografi kurva eliptik atas Galois *field* prima, maka dalam penelitian ini didefinisikan representasi simbol yang diwakili oleh huruf $A - Z$ dan $0,1, \dots, 9, +, ?$ dengan titik-titik dalam kurva eliptik yang telah diperoleh. Banyaknya karakter yang dapat direpresentasikan bergantung pada jumlah titik yang diperoleh. Adapun rincian representasi ini dapat dilihat pada Tabel

Tabel 3. Representasi Titik-titik Kurva Eliptik

Titik-titik Kurva Eliptik	Simbol	Titik-titik Kurva Eliptik	Simbol
$\theta = (3,21)$	A	$20\theta = (311,314)$	T
$2\theta = (60,95)$	B	$21\theta = (151,7)$	U
$3\theta = (223,66)$	C	$22\theta = (200,139)$	V
$4\theta = (140,304)$	D	$23\theta = (142,47)$	W
$5\theta = (9,316)$	E	$24\theta = (209,148)$	X
$6\theta = (248,32)$	F	$25\theta = (121,134)$	Y
$7\theta = (302,214)$	G	$26\theta = (44,66)$	Z
$8\theta = (216,308)$	H	$27\theta = (301,255)$	0
$9\theta = (105,230)$	I	$28\theta = (220,249)$	1
$10\theta = (288,37)$	J	$29\theta = (50,251)$	2
$11\theta = (161,236)$	K	$30\theta = (46,180)$	3
$12\theta = (242,41)$	L	$31\theta = (108,210)$	4
$13\theta = (11,168)$	M	$32\theta = (298,82)$	5
$14\theta = (180,174)$	N	$33\theta = (230.277)$	6
$15\theta = (176,39)$	O	$34\theta = (127,219)$	7
$16\theta = (34,181)$	P	$35\theta = (12,72)$	8
$17\theta = (304,307)$	Q	$36\theta = (158,263)$	9
$18\theta = (67,172)$	R	$37\theta = (20,294)$	+
$19\theta = (7,29)$	S	$38\theta = (89,127)$	?

4.4.4 Proses Enkripsi dan Dekripsi

Untuk proses enkripsi dan dekripsi menggunakan kunci privat $d = 7$, kunci publik $Q = d.G = 7.(3,21) = (302,214)$ dan nilai $k = 6$. Berikut pada Tabel 4 di bawah ini merupakan proses enkripsi dan dekripsi dari kata "MATEMATIKA":

Tabel 4. Proses enkripsi *plaintext* "MATEMATIKA"

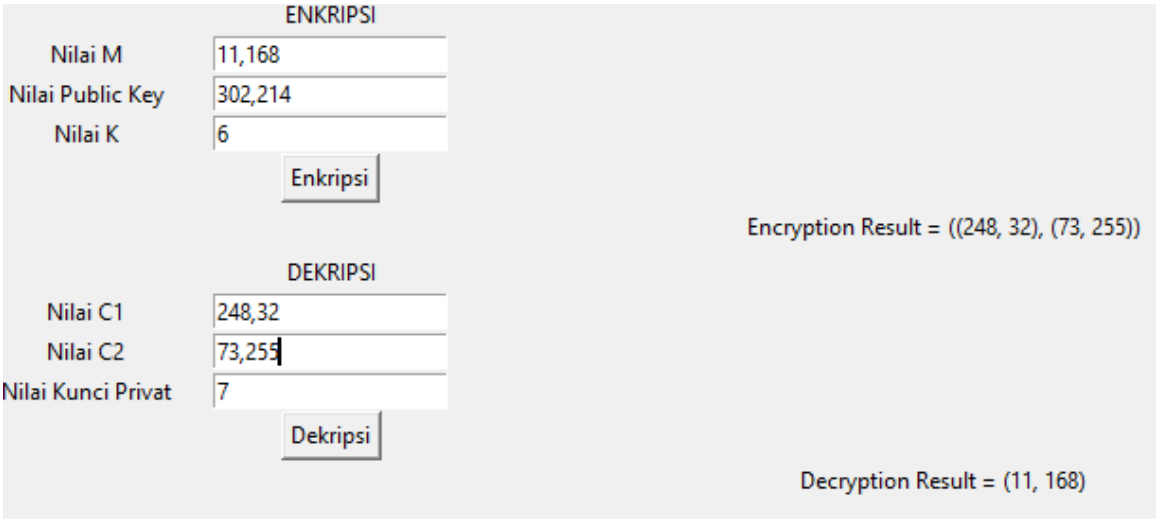
Karakter	$C_1 = k.G$	$C_2 = M + k.Q$	(C_1, C_2)
$13\theta = (11,168) = M$	(248,32)	(73,255)	[(248,32), (73,255)]
$\theta = (3,21) = A$	(248,32)	(6,196)	[(248,32), (6,196)]
$20\theta = (311,314) = T$	(248,32)	(297,217)	[(248,32), (297,217)]
$5\theta = (9,316) = E$	(248,32)	(79,264)	[(248,32), (79,264)]
$13\theta = (11,168) = M$	(248,32)	(73,255)	[(248,32), (73,255)]
$\theta = (3,21) = A$	(248,32)	(6,196)	[(248,32), (6,196)]
$20\theta = (311,314) = T$	(248,32)	(297,217)	[(248,32), (297,217)]
$9\theta = (105,230) = I$	(248,32)	(177,220)	[(248,32), (177,220)]
$11\theta = (161,236) = K$	(248,32)	(16,36)	[(248,32), (16,36)]
$\theta = (3,21) = A$	(248,32)	(6,196)	[(248,32), (6,196)]

Selanjutnya, untuk hasil dari proses dekripsi dapat dilihat pada Tabel 5 di bawah ini

Tabel 5. Proses Dekripsi

C_1	C_2	d	$M = C_2 - d.C_1$
(248,32)	(73,255)	7	$M = (73,255) - 7(248,32) = (11,168) = M$
(248,32)	(6,196)	7	$M = (6,196) - 7(248,32) = (3,21) = A$
(248,32)	(297,217)	7	$M = (297,217) - 7(248,32) = (311,314) = T$
(248,32)	(79,264)	7	$M = (79,264) - 7(248,32) = (9,316) = E$
(248,32)	(73,255)	7	$(M = (73,255) - 7(248,32) = (11,168) = M$
(248,32)	(6,196)	7	$M = (6,196) - 7(248,32) = (3,21) = A$
(248,32)	(297,217)	7	$M = (297,217) - 7(248,32) = (311,314) = T$
(248,32)	(177,220)	7	$M = (177,220) - 7(248,32) = (105,230) = I$
(248,32)	(16,36)	7	$M = (16,36) - 7(248,32) = (161,236) = K$
(248,32)	(6,196)	7	$M(6,196) - 7(248,32) = (3,21) = A$

Tampilan *Graphical User Interface* (GUI) pada proses enkripsi maupun deskripsi dengan menggunakan program yang telah dikonstruksi dapat dilihat pada Gambar 6 di bawah ini.



Gambar 6. Proses enkripsi dan dekripsi

V. KESIMPULAN

Berdasarkan hasil yang diperoleh dari penelitian ini, maka dapat disimpulkan bahwa Kriptografi kurva eliptik ElGamal yang diimplementasikan di Galois *field* prima menggunakan konsep matematika. Sistem kriptografi jenis ini merupakan sistem yang aman untuk menjaga kerahasiaan sebuah pesan atau informasi. Karena dengan perhitungan titik-titik kurva eliptik yang rumit, hal tersebut akan sangat sulit diretas keamanannya. Kemudian, implementasi kriptografi kurva eliptik ElGamal menggunakan *Python* memiliki tiga tahapan, yaitu pembentukan kunci, enkripsi dan dekripsi. Hasil pembentukan kunci diperoleh kunci publik dan kunci rahasia. Input dari proses enkripsi berupa *plaintext* yang akan dienkripsi menggunakan kunci publik dan kunci privat dengan output berupa *ciphertext*. Sementara dalam proses dekripsi input berupa *ciphertext* dan kunci privat dengan output berupa *plaintext*. Berdasarkan penelitian ini diperoleh bahwa dengan menggunakan *Python* akan lebih mempercepat proses perhitungan sistem kriptografi kurva eliptik ElGamal pada Galois *field* prima.

UCAPAN TERIMAKASIH

Penulis mengucapkan terimakasih kepada Ibu Dian Eka Wijayanti, M.Si dan Bapak Dr. Yudi Ari Adi, M.Si atas komentar dan saran sehingga penelitian ini dapat terselesaikan dengan baik.

REFERENSI

[1] B. Raharjo, Kuspriyanto, M. Paryasto, I. Muchtadi-Alamsyah, F. Yuliawan, and Nopendri, *Pengantar Kurva eliptik dan lapangan hingga*. Bandung: Penerbit Institut Teknologi Bandung, 2014.

[2] A. H. Koblitz, N. Koblitz, and A. Menezes, Elliptic Curve Cryptography: The Serpentine Course of a Paradigm Shift, *Journal of Number Theory*, vol 131, no. 5, pp. 781-814, 2011.

[3] D. Krumm and N. Sutherland, Galois Groups Over Rational Function Fields and Explicit Hilbert Irreducibility, *Journal of Symbolic Computation,* vol. 103, pp. 108-126. 2021.
[4] A. Bachmayr, D. Harbater, J. Hartmann, and M. Wibmer, The Differential Galois Group of the Rational Function Field, *Advance in Mathematics,* vol. 381, 2021.
[5] J. Wu, X. Liao, and B. Yang, Color Image Encryption Based on Chaotic Systems and Elliptic Curve ElGamal Scheme, *Signal Processing*, vol. 141, pp. 109-124, 2017.
[6] Y. Luo, X. Ouyang, J. Liu, and L. Cao, An Image Encryption Method Based on Elliptic Curve Elgamal Encryption and Chaotic Systems, *IEEE Access*, vol. 7, pp. 38507-38522, 2019.
[7] A. Abro, Z. Deng, and K. A. Memon, A Lightweight Elliptic-ElGamal-Based Authentication Scheme for Secure Device-to-Device Communication, *Future Internet*, vol. 11, no. 5, 2019
[8] M. C. Sinaga, *Kriptografi dan Python*. Medan, 2017.
[9] Litasari and B. Rahadjo, Design and Implementation Stegocrypto Based on ElGamal Elliptic Curve, in *Proceedings of the International Conference on Information Technology, Information Systems and Electrical Engineering (ICITISEE)*, pp 95-99, 2018.
[10] P. W. Prasetyo and M. Z. Riyanto, Penerapan Kurva Eliptik Atas Zp Pada Skema Tanda Tangan El Gamal, in *Prosiding Seminar Nasional Matematika Dan Pendidikan Matematika*, pp. 67–72, 2010.
[11] J. Silverman, *Advanced Topics in the Arithmetic of Elliptic Curves*. New York: Springer-Verlag, 1994.
[12] H. K. Mohanta, Secure Data Hiding using Elliptical Curve Cryptography and Steganography, *International Journal of Computer Applications*, vol. 108, no. 3, pp. 16-20, 2014.
[13] I. Halik and Y. Prayudi, Studi dan Analisis Algoritma Rivest Code 6 (RC6) dalam Enkripsi/Dekripsi Data, in *Prosiding Seminar Nasional Aplikasi Teknologi Informasi (SNATI)*, pp. 149-158, 2005.
[14] A. Zelviana, S. Efendi, and A. Dedy, Perancangan Aplikasi Pembelajaran Kriptografi Kunci Publik ElGamal Untuk Mahasiswa, *Jurnal Dunia Teknologi Informasi*, vol. 1, no. 1, pp. 56-62, 2012.