EULER: Jurnal Ilmiah Matematika, Sains dan Teknologi
Journal Homepage: http://ejurnal.ung.ac.id/index.php/Euler
DOI: https://doi.org/10.37905/euler.v11i2.23009
Desember 2023, Vol. 11, No. 2, pp. 361-371

Sistem Kriptografi Klasik Dengan Memanfaatkan Orde Dari Grup Titik Pada Kurva Eliptik Bentuk Montgomery

Yanuar Bhakti Wira Tama[1*], Muhammad Firdhausi Fahmi[2]

[1,2] Program Studi Matematika, Institut Teknologi Kalimantan, Balikpapan, Indonesia
**Penulis Korespondensi. Email: yanuar.bhakti@lecturer.itk.ac.id*

Abstrak

Kriptografi kurva eliptik merupakan salah satu bidang aplikasi dari konsep aljabar dan teori bilangan. Salah satu bentuk sistem kriptografi kurva eliptik adalah kriptografi kurva eliptik bentuk Montgomery. Dalam tulisan ini dibentuk suatu metode sistem kriptografi klasik yang terdiri dari enkripsi dan deskripsi yang terdiri dari dua puluh enam huruf alfabetik yang dipetakan ke titik-titik pada kurva eliptik dengan memanfaatkan orde dari grup titik pada kurva eliptik bentuk Montogomery. Kemudian diberikan beberapa contoh implementasi pada kasus sederhana untuk verifikasi hasil.

Kata Kunci: Dekripsi; Enkripsi; Kriptografi; Kurva Eliptik; Montgomery

Abstract

Elliptic curve cryptography is one of the application fields of algebra and number theory concepts. One form of elliptic curve cryptography is Montgomery elliptic curve cryptography. In this paper, a method for a classical cryptographic system be formulated, consisting of encryption and decryption involving twenty-six alphabetical letters which are mapped to points on an elliptic curve by utilizing the order of the point group on the Montgomery elliptic curve. Several examples of implementation in simple cases are given to verify the results.

Keywords: *Cryptography; Decryption; Elliptic Curve; Encryption; Montgomery*

1. Pendahuluan

Kriptografi merupakan salah satu bidang yang berkaitan dengan matematika atau lebih tepatnya aljabar dan teori bilangan yang tujuannya digunakan untuk menyembunyikan atau melindungi suatu informasi. Suatu kriptosistem terdiri dari lima-tupel $(\mathcal{P}, \mathcal{C}, \mathcal{K}, \mathcal{E}, \mathcal{D})$ dengan $\mathcal{P}$ merupakan himpunan *plaintext* atau pesan awal, $\mathcal{C}$ merupakan himpunan *chipertext* atau pesan tersandi, $\mathcal{K}$ merupakan kunci yang digunakan merahasiakan pesan, $\mathcal{E}$ merupakan himpunan semua kemungkinan fungsi enkripsi yang memetakan *plaintext* ke *chipertext*, sedangkan $\mathcal{D}$ merupakan semua kemungkinan fungsi deskripsi yang memetakan balik *chipertext* ke *plaintext*. Misalkan untuk suatu kunci $K \in \mathcal{K}$ terdapat suatu fungsi enkripsi $e_K: \mathcal{P} \to \mathcal{C}$ dan suatu fungsi deskripsi $d_K: \mathcal{C} \to \mathcal{P}$, sehingga untuk setiap $x \in \mathcal{P}$ berlaku $d_K(e_K(x)) = x$. Salah satu bentuk sistem kriptografi adalah kriptografi kurva eliptik yang dikenalkan Miller [1] pada tahun 1986 dan Koblitz [2] pada tahun 1987. Penggunaan kurva eliptik selain sebagai sistem kriptografi dapat digabungkan dengan beberapa hal seperti optimasi video pada IoT, steganografi, transmisi grafik [3]–[7]. Seiring dengan perkembangan ilmu, banyak muncul bentuk-bentuk kurva eliptik, salah satunya adalah kurva eliptik bentuk Montgomery. Kurva eliptik bentuk Montgomery ini diperkenalkan oleh Montgomery [8] pada tahun 1987, dengan bentuk umum kurva memenuhi persamaan (1).

$$By^2 = x^3 + Ax^2 + x \tag{1}$$

Submit: 12 November 2023, Direvisi: 14 Desember 2023, Disetujui: 16 Desember 2023

untuk suatu lapangan $\mathbb{K}$, dengan nilai $A, B \in \mathbb{K}$ dan parameter-parameternya harus memenuhi $B(A^2 - 4) \neq 0 \in \mathbb{K}$. Salah satu keunggulan dari kurva eliptik bentuk ini adalah kurva ini lebih mengutamakan koordinat-x dalam operasi titiknya. Awalnya kurva eliptik ini digunakan untuk mempercepat faktorisasi suatu bilangan, namun dari beberapa penelitian kurva bentuk ini juga dapat digunakan dalam sistem kriptografi. Salah satu contohnya adalah penggunaan pada *curve25519* yang dilakukan oleh Bernstein [9], selain itu terdapat beberapa hasil terkait pengaplikasian kurva eliptik Montgomery seperti [10]–[14]. Himpunan titik-titik yang memenuhi persamaan (1) bersama dengan titik tak hingga O membentuk suatu grup komutatif. Dengan memanfaatkan orde titik dari anggota grup akan dibentuk suatu sistem kriptografi klasik yang terdiri dari sistem enkripsi dan deskripsi.

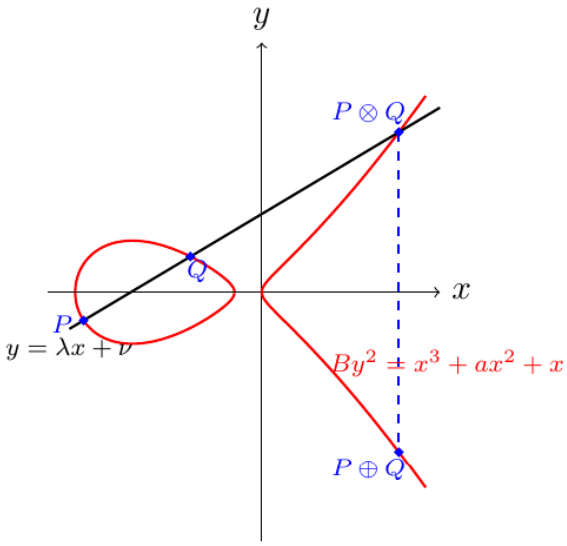
Operasi penjumlahan ($\oplus$) pada kurva eliptik awalnya didefinisikan pada himpunan bilangan real terlebih dahulu dengan menggunakan persamaan garis. Misalkan terdapat dua buah titik $P(x_1, y_1)$ dan $Q(x_2, y_2)$ dengan $x_1 \neq x_2$, bentuk suatu garis yang melalui kedua titik tersebut. Karena dari persamaan (1) terdiri dari polinom derajat tiga, maka garis tersebut memotong titik lain di kurva tersebut, sebut saja titik $P \otimes Q(x_3, -y_3)$ kemudian hasil penjumlahan titik diperoleh dengan cara mencerminkan titik $P \otimes Q(x_3, -y_3)$ terhadap sumbu-x, sehingga diperoleh hasil penjumlahannya yaitu $R(x_3, y_3) = P(x_1, y_1) \oplus Q(x_2, y_2)$, dengan nilai-nilai x_3 dan y_3 memenuhi persamaan-persamaan (2)-(4):

$$\lambda = \frac{y_2 - y_1}{x_2 - x_1} \tag{2}$$

$$x_3 = \lambda^2 - A - x_1 - x_2 \tag{3}$$

$$y_3 = \lambda(x_1 - x_3) - y_1 \tag{4}$$

Ilustrasi penjumlahan titik $P(x_1, y_1) \oplus Q(x_2, y_2)$ dapat dilihat pada Gambar 1.



Gambar 1. Ilustrasi Penjumlahan titik $P \oplus Q$

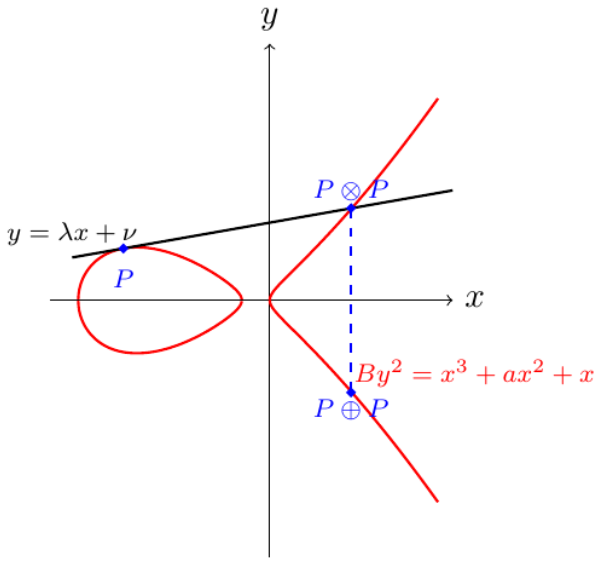
Perhatikan pada persamaan (2), penjumlahan titik tidak dapat dilakukan ketika $P = Q$ dikarenakan penyebut dari persamaan (2) bernilai nol, dengan demikian perlu didefinisikan ulang untuk penjumlahan titik yang sama. Misalkan ingin diperoleh hasil penjumlahan dari titik $P(x_1, y_1)$ dan $P(x_1, y_1)$ dengan $x_1 \neq 0$. Dengan memanfaatkan garis singgung di titik $P(x_1, y_1)$ menggunakan turunan implisit, dapat diperoleh gradien garis singgung di titik $P(x_1, y_1)$. Kemudian garis singgung yang sudah diperoleh memiliki titik perpotongan lain pada kurva yaitu $P \otimes P(x_4, -y_4)$, lalu cerminkan terhadap sumbu-x diperoleh hasil $S(x_4, y_4) = P(x_1, y_1) \oplus P(x_1, y_1) = 2 \cdot P$, dengan nilai-nilai x_4 dan y_4 memenuhi persamaan-persamaan (5)-(7).

$$\lambda = \frac{3x_1^2 + 2Ax_1 + 1}{2By_1} \tag{5}$$

$$x_4 = \lambda^2 - A - 2 \cdot x_1 \quad (6)$$

$$y_4 = \lambda(x_1 - x_4) - y_1 \quad (7)$$

Operasi penjumlahan dengan titik yang sama disebut sebagai operasi penggandaan. Ilustrasi penggandaan titik $P(x_1, y_1) \oplus P(x_1, y_1)$ dapat dilihat pada Gambar 2.



Gambar 2. Ilustrasi Penggandaan titik $P \oplus P = 2P$

Untuk operasi kasus-kasus yang lain cukup didefiniskan. Operasi-operasi yang terkait dengan balikan titik, titik tak hingga O dan titik $(0,0)$ didefinisikan pada persamaan (8)-(11).

$$O \oplus O = O \quad (8)$$

$$(x, y) \oplus (x, -y) = (x, -y) \oplus (x, y) = O \quad (9)$$

$$(x, y) \oplus O = O \oplus (x, y) = (x, y) \quad (10)$$

$$(0,0) \oplus (0,0) = O \quad (11)$$

Himpunan titik-titik kurva eliptik bentuk Montgomery ditambah dengan titik tak hingga O membentuk grup komutatif atas operasi $\oplus$ dengan identitas O, dan balikan titik (x, y) adalah $(x, -y)$. Operasi pada kurva eliptik juga dapat didefinisikan pada lapangan $\mathbb{Z}_p$ untuk p bilangan prima ganjil. Seluruh operasi kurva eliptik pada lapangan $\mathbb{Z}_p$ mirip dengan operasi pada bilangan real yang digantikan oleh operasi analog di lapangan $\mathbb{Z}_p$. Seperti operasi penjumlahan titik $P(x_1, y_1)$ dan titik $Q(x_2, y_2)$ dengan $x_1 \neq x_2$ pada persamaan (2)-(4) dapat digantikan dengan persamaan (12)-(14)

$$\lambda = (y_2 - y_1) \cdot (x_2 - x_1)^{-1} \; mod \; p \quad (12)$$

$$x_3 = (\lambda^2 - A - x_1 - x_2) \; mod \; p \quad (13)$$

$$y_3 = (\lambda(x_1 - x_3) - y_1) \; mod \; p \quad (14)$$

Untuk kasus penggandaan titik $P(x_1, y_1)$ dari persamaan (5)-(7) dapat diganti menjadi persamaan (15)-(17)

$$\lambda = (3x_1^2 + 2Ax_1 + 1) \cdot (2By_1)^{-1} \; mod \; p \quad (15)$$

$$x_4 = (\lambda^2 - A - 2 \cdot x_1) \; mod \; p \quad (16)$$

$$y_4 = (\lambda(x_1 - x_4) - y_1) \; mod \; p \quad (17)$$

Selain itu, terdapat operasi perkalian skalar pada kurva eliptik yang dapat ditulis sebagai nP. Operasi skalar tersebut menyederhanakan penjumlahan sebanyak n titik pada yang sama P, atau

$$nP = \underbrace{P \oplus P \oplus ... \oplus P}_{n\ kali} \tag{18}$$

Dalam operasi kurva eliptik jika berhadapan dengan perkalian skalar dari suatu titik membutuhkan operasi yang cukup banyak. Walaupun dapat dilakukan secara iterasi dengan aturan penjumlahan atau aturan penggadaan, namun membutuhkan waktu yang cukup lama. Karena dalam tulisan ini menggunakan kurva eliptik bentuk Montgomerry, maka dapat digunakan algoritma *Montgomery Ladder* yang dikenalkan oleh Lange [15] untuk mempercepat perkalian skalar suatu titik tersebut. Sebagai contoh, ingin diperoleh perkalian skalar $2023 \cdot P$, maka secara konvensional dapat diselesaikan dengan menjumlahkan 2023 kali titik, tentu saja hal tersebut yang ingin dihindari. Dalam algoritma *Montgomerry Ladder* ubah terlebih dahulu unsur pengali skalar menjadi bilangan biner. Kemudian dari digit terakhir apakah digit bernilai 0 atau 1, lalu gunakan operasi-operasi penjumlahan atau penggandaan titik yang sudah disebutkan sebelumnya. kemudian ikuti Algoritma di bawah:

Algorithm 1: Montgomery Ladder

Input : Point P, scalar n
Output: nP

$R_0 \leftarrow \mathcal{O}$
$R_1 \leftarrow P$
for $i \leftarrow m$ **downto** 0 **do**
  if $d_i = 1$ **then**
    $R_0 \leftarrow R_0 + R_1$
    $R_1 \leftarrow R_1 + R_1$
  else
    $R_1 \leftarrow R_0 + R_1$
    $R_0 \leftarrow R_0 + R_0$
  end
end
Return R_0;

Gambar 3. Algoritma Montgomerry Ladder

Dengan demikian, untuk bilangan 2023 dapat diubah menjadi dalam notasi bilangan biner menjadi 11111100111_2 atau bilangan biner dengan 11 digit. Dengan menggunakan algoritma *Montgomery ladder* cukup dengan menggunakan 11 kali iterasi algoritma atau total 22 operasi, berbeda jauh dengan cara konvensional yaitu 2023.

Dalam suatu grup berhingga G dengan identitas e, untuk suatu $a \in G$ bilangan asli terkecil n yang memenuhi $n \cdot a = e$ disebut orde dari a. Sedangkan banyaknya anggota dari G disebut sebagai order dari grup G. Dalam grup titik kurva eliptik dengan identitas O, setiap titik mempunyai orde. Orde dari titik P pada kurva eliptik berorde n, jika memenuhi $nP = O$. Sebagai contoh, titik O akan berorde 1 karena merupakan identitas, sedangkan titik $(0,0)$ akan berorde 2 karena telah didefinisikan $(0,0) \oplus (0,0) = O$.

Sistem enkripsi dan dekripsi yang digunakan dalam tulisan ini memanfaatkan orde dari setiap elemen kurva eliptik pada persamaan (1). Dalam sistem kriptografi ini menggunakan *plaintext* ($\mathcal{P}$) dan *chipertext* ($\mathcal{C}$) huruf alfabet A-Z. Untuk enkripsi (e_K) gunakan kunci privat $K = n_b$ yang saling prima dengan order grup kurva eliptik, lalu kalikan pada suatu *plaintext* $p \in P$ seperti pada persamaan (19).

$$e_K(p) = n_b \cdot p \tag{19}$$

Sedangkan pada deskripsi pesan (d_K) pilih suatu nilai m_b, sehingga perkalian dari m_b dan n_b menghasilkan 1 dalam modulo o_i dengan o_i merupakan setiap orde dari anggota titik di kurva eliptik. Hal itu dilakukan untuk memastikan bahwa perkalian skalar yang dipilih untuk enkripsi mempunyai balikan, sehingga jika dikalikan menghasilkan 1. Untuk suatu *chipertext* $c \in C$ kalikan dengan m_b, sehingga diperoleh hasil persamaan (20).

$$d_K(c) = m_b \cdot c = m_b \cdot (n_b \cdot p) = m_b \cdot n_b \cdot p = p \tag{20}$$

Tulisan ini bertujuan untuk membuat sistem kriptografi yang terdiri dan enkripsi dan dekripsi pesan dengan memanfaatkan orde dari anggota titik pada kurva eliptik bentuk Montgomerry. Kurva eliptik didefinisikan atas lapangan hingga $\mathbb{Z}_p$ untuk suatu bilangan prima p. Himpunan *Plaintext* dan *Chipertext* sistem ini menggunakan dua puluh enam huruf alfabetik. Terakhir, implementasi sederhana untuk verifikasi hasil teori yang sudah diusulkan.

2. Metode Penelitian

Penelitian ini dilaksanakan dengan metode studi literatur. Tahapan penelitian dapat dilihat pada Gambar 4.

Gambar 4. Diagram Tahap Penelitian

Tahap-tahap penelitian dari Gambar 4 dapat

1. Menentukan parameter-parameter kurva eliptik bentuk Montgomery yang terdiri dari banyak koordinat-x yang berbeda sebanyak dua puluh enam.
2. Tentukan orde dari setiap titik pada kurva eliptik yang digunakan.
3. Petakan titik-titik pada kurva eliptik ke setiap huruf alfabetik berdasarkan orde titik.
4. Pilih kunci enkripsi dan dekripsi yang sesuai, kemudian implementasi dengan beberapa contoh sederhana untuk memverifikasi sistem kriptogtafi klasik.
5. Penarikan kesimpulan dari penelitian.

3. Hasil dan Pembahasan

Berdasarkan metode yang telah dipaparkan, bagian hasil dan pembahasan dibagi menjadi empat bagian yaitu, pemilihan parameter kurva eliptik, perhitungan orde titik, pemetaan titik, dan implementasi. Dalam hal ini hanya dipilih satu pemilihan parameter saja karena berfokus pada penggunaan kurva eliptik untuk sistem kriptografi klasik yang biasanya digunakan dalam kriptografi kunci publik.

3.1 Pemilihan Parameter Kurva Eliptik

Agar diperoleh himpunan *plaintext* dan *chipertext* yang terdiri dari 26 huruf alfabetik haruslah himpunan titik tersebut terdiri dari 26 titik, atau mempunyai subgrup berorde 26, atau banyaknya koordinat-x yang berbeda ada 26. Dalam penulisan ini dipilih kurva eliptik Montgomery dengan parameter $A = 5$ dan $B = 1$ atas lapangan hingga $\mathbb{Z}_{37}$, atau persamaan kurva eliptik yang digunakan memenuhi persamaan (21).

$$y^2 \equiv x^3 + 5x^2 + x \; mod \; 37 \tag{21}$$

Banyaknya titik yang memenuhi persamaan (21) sebanyak 48 titik, dengan koordinat-x yang berbeda terdapat 26 titik. Nilai koordinat-x yang memenuhi persamaan (21) selain titik O adalah 0,1,2,3,4,5,7,8,9,10,13,14,15,16,17,18,19,20,24,25,26,28,33,35, dan 36.

3.2 Perhitungan Orde Titik

Karena titik O merupakan identitas grup, maka dalam menentukan orde titik P cukup jumlahkan titik P terus menerus sampai diperoleh titik O. Sebagai contoh, jika diambil titik $P(1,9)$ pada kurva eliptik tersebut diperoleh

1. Untuk penjumlahan $P \oplus P = 2P$ atau penggandaan dari persamaan (15)-(17) diperoleh

$$\lambda = (3 + 10 + 1) \cdot (18)^{-1} \; mod \; 37 = 9 \; mod \; 37$$
$$x = (9^2 - 5 - 2) \; mod \; 37 = 0 \; mod \; 37$$
$$y = (9(1 - 0) - 9) \; mod \; 37 = 0 \; mod \; 37$$

   Diperoleh hasil penggandannya adalah $(0,0)$.

2. Untuk penjumlahan $2P(0,0) \oplus P(1,9) = 3P$ dengan menggunakan persamaan (12)-(14) diperoleh

$$\lambda = (9 - 0) \cdot (1 - 0)^{-1} \; mod \; 37 = 9 \; mod \; 37$$
$$x = (9^2 - 5 - 1 - 0) \; mod \; 37 = 1 \; mod \; 37$$
$$y = (9(0 - 1) - 0) mod \; 37 = -9 \; mod \; 37 = 28 \; mod \; 37$$

   Diperoleh hasil penjumlahannya adalah $(1, -9)$ atau ekivalen dengan $(1,28)$

3. Kemudian jumlahkan lagi $3P(1,28) \oplus P(1,9) = 4P$. Berdasarkan pendefinisian operasi pada persamaan (9) diperoleh $4P = O$.

   Dengan demikian dapat disimpulkan bahwa titik $(1,9)$ berorde 4.

Daftar titik-titik yang telah diperoleh dari pemilihan parameter kurva eliptik pada persamaan (21) beserta orde dari elemen grup-nya dapat dilihat pada Tabel 1.

Tabel 1. Tabel orde elemen grup kurva eliptik

Titik	O	(0,0)	(1,9) (1,28)	(2,17) (2,20)	(3,1) (3,36)	(4,0)	(5,12) (5,25)	(7,15) (7,22)	(8,10) (8,27)
Orde	1	2	4	8	12	2	8	3	24
Titik	(9,12) (9,25)	(10,17) (10,22)	(13,13) (13,24)	(14,1) (14,36)	(15,1) (15,36)	(16,8) (16,29)	(17,14) (17,23)	(18,12) (18,25)	(19,5) (19,32)
Orde	6	12	24	24	24	8	24	24	12
Titik	(20,17) (20,20)	(24,2) (24,35)	(25,4) (25,33)	(26,15) (26,22)	(28,0)	(33,7) (33,30)	(35,11) (35,26)	(36,15) (36,22)	
Orde	12	24	12	12	2	6	24	4	

Dari Tabel 1 orde titik-titik yang mungkin adalah 1,2,3,4,8,12, dan 24. Untuk pemilihan kunci harus memenuhi persamaan (22)-(23)

$$FPB(n_b, 24) = 1 \tag{22}$$
$$n_b \cdot m_b = 1 \; mod \; o_i \tag{23}$$

dengan n_b dan m_b masing-masing menyatakan kunci untuk enkripsi dan dekripsi, sedangkan o_i menyatakan orde dari grup selain 1. Dengan demikian, pasangan-pasangan yang mungkin adalah

$$(n_b, m_b) = \{(1,1); (5,5), (7,7), (11,11), (13,13), (17,17), (19,19), (23,23)\}$$

3.3 Pemetaan Titik

Berdasarkan dua puluh enam huruf dalam alfabetik yang digunakan, petakan setiap titik koordinat-x dengan aturan frekuensi yang sering muncul dipetakan ke koordinat-x dengan orde tertinggi yaitu 24 sampai frekuensi yang jarang muncul dipetakan ke koordinat-x dengan orde terendah berdasarkan hasil dari Grigas [16], hasil pemetaan dapat dilihat pada Tabel 2.

Tabel 2. Tabel pemetaan huruf ke titik kurva eliptik

Huruf	A	B	C	D	E	F	G	H	I
Titik	(24,2) (24,35)	(36,15) (36,22)	(19,5) (19,32)	(20,17) (20,20)	(35,11) (35,26)	(16,8) (16,29)	(2,17) (2,20)	(26,15) (26,22)	(17,14) (17,23)
Huruf	J	K	L	M	N	O	P	Q	R
Titik	(4,0)	(7,15) (7,22)	(25,4) (25,33)	(3,1) (3,36)	(14,1) (14,36)	(15,1) (15,36)	(5,12) (5,25)	O	(8,10) (8,27)
Huruf	S	T	U	V	W	X	Y	Z	
Titik	(13,13) (13,24)	(18,12) (18,25)	(10,17) (10,22)	(1,9) (1,28)	(33,7) (33,30)	(28,0)	(9,12) (9,25)	(0,0)	

3.4 Implementasi Sistem Kriptografi

Setelah semua titik sudah dipetakan ke masing-masing huruf alfabetik, sudah saatnya dapat diimplementasikan sistem kriptografi klasik dengan menggunakan kurva eliptik tersebut. Perhatikan bahwa, dalam penggunaan sistem kriptografi klasik ini tidak hanya menggunakan teori bilangan saja seperti kriptografi klasik lainnya, namun juga digunakan beberapa konsep aljabar terkait grup dan lapangan, sehingga hasilnya tidak terlihat membentuk pola seperti kriptografi klasik yang menggunakan teori bilangan saja. Pertama, pilih kunci privat $n_b = 5$ akibatnya berdasarkan persamaan (22)-(23) nilai yang mungkin untuk m_b adalah 5. Sebagai contoh penerapan sistem enkripsi dan deskripsi ini dengan nilai n_b dan m_b yang terpilih dicoba dengan kata "MATEMATIKA". Misalkan Alice ingin mengirimkan pesan tersebut kepada Bob maka terdapat kemungkinan 2^{10} titik yang dipilih. Pilih salah satu kombinasi titik yang mungkin dan enkripsi pesannya dengan perkalian skalar $n_b = 5$.

Dalam mengenkripsi setiap karakter dapat menggunakan algoritma *Montgomerry Ladder*. Karena angka 5 mempunyai bentuk representatif biner 101 maka terdapat 3 buah langkah algoritma. Jika mengikuti langkah-langkah dari algoritma *Montgomerry Ladder* dapat dilihat dalam sistem perkalian skalar titik yang merepresentasikan huruf M yaitu titik (3,1) diperoleh hasil:

1. Inisiasi titik pertama $R_0 = O$ dan $R_1 = (3,1)$
2. Karena digit terakhirnya 1, maka $R_0 = R_0 + R_1 = (3,1)$ dan $R_1 = 2 \cdot R_1 = (16,29)$
3. Digit ke-2 nya adalah 0, maka $R_0 = R_0 + R_0 = (16,29)$ dan $R_1 = R_0 + R_1 = (1,9)$
4. Digit pertamanya adalah 1, maka $R_0 = R_0 + R_1 = (25,33)$ dan $R_1 = 2 \cdot R_1 = (0,0)$
5. Ambil nilai dari R_0 lalu simpan sebagai hasil dari $5 \cdot P$

Dari penggunaan algoritma *Montgomerry Ladder* titik (3,1) yang berkorespondensi dengan huruf M menghasilkan titik $5P(25,33)$ yang berkorespondensi pada Tabel 2 merupakan huruf L. Jika semua pesan dikenakan algoritma *Montgomerry Ladder* diperoleh hasil enkripsi dari kata "MATEMATIKA" seperti pada Tabel 3.

Tabel 3. Contoh Enkripsi Pesan MATEMATIKA

Pesan	M	A	T	E	M	A	T	I	K	A
P	(3,1)	(24,2)	(18,12)	(35,11)	(3,36)	(24,35)	(18,25)	(17,14)	(7,15)	(24,2)
$5 \cdot P$	(25,33)	(18,12)	(24,2)	(17,23)	(25,4)	(18,25)	(24,35)	(35,26)	(7,22)	(18,12)
Chiper	L	T	A	I	L	T	A	E	K	T

Dari hasil Tabel 3 dapat dilihat bahwa untuk karakter yang sama yaitu huruf M yang menggunakan inisiasi yang berbeda yaitu (3,1) dan (3,36) diperoleh hasil enkripsi berturut-turut adalah titik (25,33) dan (25,4) yang mempunyai koordinat-x yang sama. Begitu juga dengan huruf A yang menggunakan titik (24,2) dan (24,35) diperoleh hasil enkripsi berturut-turut adalah (18,12) dan (18,25) yang juga mempunyai koordinat-x yang berkorespondensi dengan huruf T. Kasus serupa juga ditemukan pada huruf T. Diperoleh hasil enkripsi pesan "MATEMATIKA" dari Alice kepada Bob adalah "LTAILATEKT".

Kemudian untuk deskripsi pesan dari suatu *chipertext* gunakan $m_b = 5$, nilai tersebut dipilih karena memenuhi

$$n_b \cdot m_b = 1 \; mod \; 2$$
$$n_b \cdot m_b = 1 \; mod \; 3$$
$$n_b \cdot m_b = 1 \; mod \; 4$$
$$n_b \cdot m_b = 1 \; mod \; 6$$
$$n_b \cdot m_b = 1 \; mod \; 8$$
$$n_b \cdot m_b = 1 \; mod \; 12$$
$$n_b \cdot m_b = 1 \; mod \; 24$$

Setelah Bob mendapatkan pesan enkripsi dari Alice, Bob menggunakan perkalian skalar dengan $m_b = 5$ pada *chipertext* yang diterima. Untuk mendeskripsi pesan sebelumnya dapat dilakukan dengan algoritma *Montgomerry Ladder*. Karena angka 5 mempunyai bentuk representatif biner 101 maka terdapat 3 buah langkah algoritma. Jika mengikuti langkah-langkah dari Algoritma *Montgomerry Ladder* dapat dilihat dalam sistem perkalian skalar titik (25,33).

1. Inisiasi titik pertama $R_0 = O$ dan $R_1 = (25,33)$
2. Karena digit terakhirnya 1, maka $R_0 = R_0 + R_1 = (25,33)$ dan $R_1 = 2 \cdot R_1 = (16,8)$
3. Digit ke-2 nya adalah 0, maka $R_0 = 2 \cdot R_0 = (16,8)$ dan $R_1 = R_0 + R_1 = (1,9)$
4. Digit ke-1 nya adalah 1, maka $R_0 = R_0 + R_1 = (3,1)$ dan $R_1 = 2 \cdot R_1 = (0,0)$
5. Ambil nilai dari R_0 lalu simpan sebagai hasil dari $5 \cdot C$

Hasil deskripsi dari huruf L tersebut adalah huruf yang berkorespondensi dengan titik $5C(3,1)$ yaitu huruf M berdasarkan Tabel 2. Jika semua pesan dikenakan algoritma *Montogomerry Ladder* diperoleh hasil enkripsi dari "LTAILAEKT" seperti terlihat pada Tabel 4.

Tabel 4. Contoh Dekripsi Pesan LTAILAEKT

Chiper	L	T	A	I	L	T	A	E	K	T
C	(25,33)	(18,12)	(24,2)	(17,23)	(25,4)	(18,25)	(24,35)	(35,26)	(7,22)	(18,12)
$5 \cdot C$	(3,1)	(24,2)	(18,12)	(35,11)	(3,36)	(24,35)	(18,25)	(17,14)	(7,15)	(24,2)
Pesan	M	A	T	E	M	A	T	I	K	A

Dapat diperoleh bahwa hasil deskripsi titik (25,33) kembali ke titik awalnya yaitu titik (3,1). Titik (25,3) termasuk titik yang mempunyai orde 12, perlu dilakukan verifikasi tambahan untuk titik hasil enkripsi yang mempunyai orde selain 12. Pilih hasil enkripsi titik (18,12) yang mempunyai orde 24.

1. Inisiasi titik pertama $R_0 = O$ dan $R_1 = (18,12)$
2. Karena digit terakhirnya 1, maka $R_0 = R_0 + R_1 = (18,12)$ dan $R_1 = 2 \cdot R_1 = (3,1)$
3. Digit ke-2 nya adalah 0, maka $R_0 = 2 \cdot R_0 = (3,1)$ dan $R_1 = R_0 + R_1 = (2,17)$
4. Digit ke-1 nya adalah 1, maka $R_0 = R_0 + R_1 = (24,2)$ dan $R_1 = 2 \cdot R_1 = (1,9)$

5. Ambil nilai dari R_0 lalu simpan sebagai hasil dari $5 \cdot C$

Hasil deskripsi pesan Alice yang dibaca Bob adalah "MATEMATIKA".

Untuk mengecek ulang sistem ini, gunakan kunci privat yang lain yaitu $n_b = 11$ yang mempunyai pasangan $m_b = 11$. Penerapan sistem enkripsi dan deskripsi ini menggunakan kata "INDONESIA". Pilih salah satu kombinasi titik yang mungkin dan hasil enkripsi dengan $n_b = 11$ seperti dilihatkan pada Tabel 5.

Tabel 5. Contoh Enkripsi Pesan INDONESIA

Pesan	I	N	D	O	N	E	S	I	A
P	(17,14)	(14,1)	(20,17)	(15,1)	(14,36)	(35,11)	(13,13)	(17,23)	(24,2)
$11 \cdot P$	(24,2)	(16,8)	(35,26)	(5,12)	(16,29)	(18,25)	(20,17)	(24,35)	(17,14)
Chiper	A	F	E	P	F	T	D	A	I

Hasil enkripsi dari Tabel 5 dapat dilakukan dengan algoritma *Montgomerry Ladder*. Karena angka 11 mempunyai bentuk representatif biner 1011 maka terdapat 4 buah langkah algoritma. Jika mengikuti langkah-langkah dari Algoritma *Montgomerry Ladder* dapat dilihat dalam sistem perkalian skalar titik (17,14).

1. Inisiasi titik pertama $R_0 = O$ dan $R_1 = (17,14)$
2. Karena digit terakhirnya 1, maka $R_0 = R_0 + R_1 = (17,14)$ dan $R_1 = 2 \cdot R_1 = (25,33)$
3. Digit ketiganya adalah 1, maka $R_0 = R_0 + R_1 = (2,17)$ dan $R_1 = 2 \cdot R_1 = (16,8)$
4. Digit keduanya adalah 0, maka $R_0 = R_0 + R_0 = (1,9)$ dan $R_1 = R_0 + R_1 = (18,25)$
5. Digit pertamanya adalah 1, maka $R_0 = R_0 + R_1 = (24,2)$ dan $R_1 = 2 \cdot R_1 = (3,36)$
6. Ambil nilai dari R_0 lalu simpan sebagai hasil dari $11 \cdot P$

Diperoleh hasil enkripsi titik $(17,14)$ menjadi titik $(24,2)$. Jika algoritma dilakukan pada huruf lain diperoleh hasil enkripsi kata "INDONESIA" menjadi "AFEPFTDEI".

Setelah Bob mendapatkan pesan enkripsi dari Alice, Bob menggunakan perkalian skalar dengan $m_b = 11$ pada *chipertext* yang diterima, hasil dekripsi pesannya dapat dilihat pada Tabel 6.

Tabel 6. Contoh Dekripsi Pesan AFEPFTDEI

Chiper	A	F	E	P	F	T	D	E	I
C	(24,2)	(16,8)	(35,26)	(5,12)	(16,29)	(18,25)	(20,17)	(24,35)	(17,14)
$11 \cdot C$	(17,14)	(14,1)	(20,17)	(15,1)	(14,36)	(35,11)	(13,13)	(17,23)	(24,2)
Pesan	I	N	D	O	N	E	S	I	A

Hasil dekripsi dari Tabel 6 dapat dilakukan juga dengan algoritma *Montgomerry Ladder* dengan $m_b = 11$. Sebagai contoh, deskripsikan titik $(20,17)$ atau huruf D. Karena angka 11 mempunyai bentuk representatif biner 1011 maka terdapat 4 buah langkah algoritma. Jika mengikuti langkah-langkah dari algoritma *Montgomerry Ladder* dapat dilihat dalam sistem perkalian skalar titik (20,17).

1. Inisiasi titik pertama $R_0 = O$ dan $R_1 = (20,17)$
2. Karena digit terakhirnya 1, maka $R_0 = R_0 + R_1 = (20,17)$ dan $R_1 = 2 \cdot R_1 = (3,36)$
3. Digit ketiganya adalah 1, maka $R_0 = R_0 + R_1 = (5,25)$ dan $R_1 = 2 \cdot R_1 = (16,8)$
4. Digit keduanya adalah 0, maka $R_0 = R_0 + R_0 = (1,28)$ dan $R_1 = R_0 + R_1 = (14,36)$
5. Digit pertamanya adalah 1, maka $R_0 = R_0 + R_1 = (13,13)$ dan $R_1 = 2 \cdot R_1 = (25,33)$
6. Ambil nilai dari R_0 lalu simpan sebagai hasil dari $11 \cdot P$

Hasil deskripsi pesan dari titik $(20,17)$ adalah titik $(13,13)$ atau huruf yang bersesuaian adalah huruf S. Jika titik lain diperlakukan dengan algoritma yang sama diperoleh hasil dekripsi pesan yang dibaca oleh Bob adalah "INDONESIA".

4. Kesimpulan

Hasil penelitian menghasilkan suatu sistem kriptografi klasik untuk enkripsi dan deskripsi sederhana dengan *plaintext* dan *chipertext* terdiri dari 26 huruf alfabetik. Proses enkripsi dan deskripsi memanfaatkan orde dari titik pada grup kurva eliptik bentuk Montgomery. Implementasi dari dua kasus sederhana juga sudah dilakukan dengan hasil yang sudah sesuai dengan teori yang diberikan.

Referensi

[1] V. S. Miller, "Use of Elliptic Curves in Cryptography," in *LNCS*, 1986, pp. 417–426.

[2] N. Koblitz, "Elliptic Curve Cryptosystems," *Math Comput*, vol. 48, pp. 203–209, 1987.

[3] B. S. A. Alhayani *et al.*, "Optimized video internet of things using elliptic curve cryptography based encryption and decryption," *Computers and Electrical Engineering*, vol. 101, Jul. 2022, doi: 10.1016/j.compeleceng.2022.108022.

[4] E. Hureib, A. Gutub, E. S. Bin Hureib, and A. A. Gutub, "Enhancing Medical Data Security via Combining Elliptic Curve Cryptography and Image Steganography," *IJCSNS International Journal of Computer Science and Network Security*, vol. 20, no. 8, 2020, [Online]. Available: https://www.researchgate.net/publication/344311992

[5] R. I. Abdelfatah, "Secure Image Transmission Using Chaotic-Enhanced Elliptic Curve Cryptography," *IEEE Access*, vol. 8, pp. 3875–3890, 2020, doi: 10.1109/ACCESS.2019.2958336.

[6] S. Di Matteo, L. Baldanzi, L. Crocetti, P. Nannipieri, L. Fanucci, and S. Saponara, "Secure elliptic curve crypto-processor for real-time iot applications," *Energies (Basel)*, vol. 14, no. 15, Aug. 2021, doi: 10.3390/en14154676.

[7] M. Alkhatib, "High-Speed and Secure Elliptic Curve Cryptosystem for Multimedia Applications ECC Elliptic Curve Cryptosystem RLA Right to Lift Algorithm SPA Simple Power Attack STA Simple Time Attack SM Sequential Multiplication SA Sequential Addition PM Parallel Multiplier TSM Time-consumption for one sequential multiplication TM Time-consumption for one multiplication operation TKP Time-consumption for scaler multiplication GF Galious Field NAF Non-Adjacent-Form," (*IJACSA*) *International Journal of Advanced Computer Science and Applications*, vol. 11, no. 9, 2020.

[8] P. L. Montgomery, "Speeding the Pollard and Elliptic Curve Methods of Factorization," *Math Comput*, vol. 48, pp. 243–264, 1987.

[9] D. J. Bernstein, "Curve25519: new Diffie-Hellman speed records", in *Public Key Cryptography-PKC 2006: 9th International Conference on Theory and Practice in Public-Key Cryptography, New York, NY, USA*, 2006, pp. 207–228.

[10] K. Okeya, H. Kurumatani, and K. Sakurai, "Elliptic Curves with the Montgomery-Form and Their Cryptographic Applications," in *Public Key Cryptography: Third International Workshop on Practice and Theory in Public Key Cryptosystems*, 2000, pp. 238–257. doi: doi.org/10.1007/978-3-540-46588-1_17.

[11] T. Oliveira, J. López, and F. Rodríguez-Henríquez, "The Montgomery ladder on binary elliptic curves," *J Cryptogr Eng*, vol. 8, pp. 241–258, 2018, doi: doi.org/10.1007/s13389-017-0163-8.

[12] I. Muchtadi-Alamsyah, Y. Bhakti, and W. Tama, “Implementation of Elliptic Curve25519 in Cryptography”, in *Theorizing STEM Education in the 21st Century*, 2020, p. 189. [Online]. Available: www.intechopen.com

[13] D. Basu Roy and D. Mukhopadhyay, “High-Speed Implementation of ECC Scalar Multiplication in GF(p) for Generic Montgomery Curves,” *IEEE Trans Very Large Scale Integr VLSI Syst*, vol. 27, no. 7, pp. 1587–1600, Jul. 2019, doi: 10.1109/TVLSI.2019.2905899.

[14] A. M. Awaludin, H. T. Larasati, and H. Kim, “High-Speed and Unified ECC Processor for Generic Weierstrass Curves over GF(p) on FPGA,” *Sensors*, vol. 21, no. 4, p. 1451, Feb. 2021, doi: 10.3390/s21041451.

[15] D. J. Bernstein and T. Lange, “Montgomery curves and the Montgomery ladder,” *Cryptology ePrint Archive*, vol. 293, 2017. Accessed: Nov. 12, 2023. [Online]. Available: http://eprint.iacr.org/2017/293

[16] G. Grigas and A. Juškevičienė, “Letter Frequency Analysis of Languages Using Latin Alphabet,” *International Linguistics Research*, vol. 1, no. 1, p. p18, Mar. 2018, doi: 10.30560/ilr.v1n1p18.