Analisis Kombinatorial Pada Pengkodean dan Dekode Galois

Dimas Bagoes Hendrianto - 13522112
Program Studi Teknik Informatika
Sekolah Teknik Elektro dan Informatika
Institut Teknologi Bandung, Jl. Ganesha 10 Bandung 40132, Indonesia
13522112@itb.ac.id

***Abstrak*—Pengkodean dan dekode merupakan elemen kunci dalam proses komunikasi digital yang melibatkan transformasi informasi menjadi format yang dapat ditransmisikan, dan kemudian dikembalikan ke bentuk semula. Pengkodean data memainkan peran sentral dalam mengurangi ukuran file dan meningkatkan efisiensi pengiriman data melalui jaringan. Dalam konteks komunikasi keamanan, enkripsi menjadi aspek kunci untuk melindungi informasi dari akses yang tidak sah.**

***Kata kunci*—Pengkodean, Dekode, Efisiensi, Galois**

I. PENDAHULUAN

Pada era modern yang terus berkembang pesat, kemajuan teknologi telah mengubah fundamental cara kita berinteraksi, berkomunikasi, dan menyimpan informasi. Transformasi ini membawa dampak positif dalam meningkatkan efisiensi dan keterhubungan global, namun juga memunculkan tantangan baru terkait keamanan data. Seiring dengan perkembangan teknologi, pentingnya melindungi informasi sensitif dari akses yang tidak sah dan manipulasi semakin mendesak. Inilah dimana kriptografi, sebagai ilmu keamanan informasi, mendapatkan posisi sentral dalam memastikan keamanan data di era digital.

Seiring perkembangan teknologi, ancaman terhadap keamanan data juga semakin kompleks. Serangan siber, pencurian identitas, dan spionase digital menjadi ancaman nyata yang dapat merugikan individu, perusahaan, dan bahkan negara. Oleh karena itu, kebutuhan akan metode keamanan yang dapat melindungi data dari risiko tersebut menjadi semakin mendesak. Kriptografi menjadi salah satu alat utama yang dapat memberikan lapisan perlindungan yang diperlukan dalam lingkungan digital yang penuh risiko.

Kriptografi adalah suatu disiplin ilmu yang berkaitan dengan keamanan informasi, yang bertujuan untuk melindungi data dan komunikasi dari akses yang tidak sah atau modifikasi selama proses pengiriman. Kriptografi telah menjadi elemen kritis dalam keamanan informasi di berbagai sektor, termasuk telekomunikasi, keuangan, e-commerce, dan banyak lagi. Tujuan utama kriptografi adalah menjaga kerahasiaan, integritas, dan otentikasi data.

Perkembangan teknologi membawa perubahan besar dalam kehidupan kita, namun di tengah kemudahan tersebut, keamanan data menjadi prioritas utama. Kriptografi, sebagai payung keamanan digital, memberikan solusi yang efektif dan andal untuk melindungi informasi sensitif dari ancaman di dunia maya. Pentingnya kriptografi tidak hanya sejalan dengan kemajuan teknologi, tetapi juga menjadi landasan untuk membangun kepercayaan dalam pertukaran informasi elektronik di dunia yang semakin terhubung ini. Pada makalah ini akan dibahas analisa kombinatorik pada pengkodean galois.

II. LANDASAN TEORI

A. Teori Bilangan

Teori bilangan menjadi salah satu teori yang mendasari pemahaman kriptografi, khususnya teori bilangan bulat. Teori bilangan bulat dalam matematika diskrit memberikan penekanan dengan sifat pembagian. Sifat pembagian pada bilangan bulat melahirkan konsep-konsep seperti bilangan prima dan aritmetika modulo. Satu algoritma penting yang berhubungan dengan sifat pembagian ini adalah algoritma Euclidean. Bilangan prima, aritmetika modulo, dan algoritma Euclidean memainkan peran yang penting dalam ilmu kriptografi.

1. Bilangan Bulat

Bilangan bulat adalah bilangan yang tidak mempunyai pecahan desimal, misalnya 8, 21, 8765, -34, 0. Berlawanan dengan bilangan bulat adalah bilangan riil yang mempunyai titik desimal, seperti 8.0, 34.25, 0.02.

2. Sifat Pembagian pada Bilangan Bulat

Misalkan a dan b adalah dua buah bilangan bulat dengan syarat a ¹ 0. Kita menyatakan bahwa a habis membagi b (a divides b) jika terdapat bilangan bulat c sedemikian sehingga b = ac. · Notasi: a | b jika b = ac, c Î Z dan a ¹ 0. (Z = himpunan bilangan bulat) · Kadang-kadang pernyataan “a habis membagi b“ ditulis juga “b kelipatan a”.

3. Bilangan Prima

Bilangan bulat positif p (p > 1) disebut bilangan prima jika pembaginya hanya 1 dan p. · Contoh adalah bilangan prima karena ia hanya habis dibagi oleh 1 dan 23. · Karena bilangan prima harus lebih besar dari 1, maka barisan bilangan prima dimulai dari 2, yaitu 2, 3, 5, 7, 11, 13, …. Seluruh bilangan prima adalah bilangan ganjil, kecuali 2 yang merupakan bilangan genap. · Bilangan selain prima disebut bilangan komposit (composite). Misalnya 20 adalah bilangan komposit karena 20 dapat dibagi oleh 2, 4, 5, dan 10, selain 1 dan 20 sendiri.

B. Teorema Euclidean

Misalkan m dan n adalah dua buah bilangan bulat dengan syarat n > 0. Jika m dibagi dengan n maka terdapat dua buah bilangan bulat unik q (quotient) dan r (remainder), sedemikian sehingga m = nq + r (1) dengan $0 \leq r < n$.

1. Pembagi Bersama Terbesar (PBB)

Misalkan a dan b adalah dua buah bilangan bulat tidak nol. Pembagi bersama terbesar (PBB – greatest common divisor atau gcd) dari a dan b adalah bilangan bulat terbesar d sedemikian sehingga d | a dan d | b. Dalam hal ini kita nyatakan bahwa PBB(a, b) = d.

2. Algoritma Euclidean

Algoritma Euclidean adalah algoritma untuk mencari PBB dari dua buah bilangan bulat. · Euclid, penemu algoritma Euclidean, adalah seorang matematikawan Yunani yang menuliskan algoritmanya tersebut dalam bukunya yang terkenal, Element. · Diberikan dua buah bilangan bulat tak-negatif m dan n (m ≥ n). Algoritma Euclidean berikut mencari pembagi bersama terbesar dari m dan n. Jika n = 0 maka m adalah PBB(m, n) maka berhenti. Tetapi jika $n \neq 0$, lanjutkan bagilah m dengan n dan misalkan r adalah sisanya. Ganti nilai m dengan nilai n dan nilai n dengan nilai r, lalu ulang kembali ke langkah awal.

3. Relatif Prima

Dua buah bilangan bulat a dan b dikatakan relatif prima jika PBB(a, b) = 1. Jika a dan b relatif prima, maka terdapat bilangan bulat m dan n sedemikian sehingga ma + nb = 1

C. Aritmetika Modulo

Misalkan a adalah bilangan bulat dan m adalah bilangan bulat > 0. Operasi a mod m (dibaca “a modulo m”) memberikan sisa jika a dibagi dengan m. · Notasi: a mod m = r sedemikian sehingga a = mq + r, dengan $0 \leq r < m$. Bilangan m disebut modulus atau modulo, dan hasil aritmetika modulo m terletak di dalam himpunan {0, 1, 2, …, m – 1}

1. Kongruen

Misalnya 38 mod 5 = 3 dan 13 mod 5 = 3, maka kita katakan $38 \equiv 13 \pmod 5$ (baca: 38 kongruen dengan 13 dalam modulo 5). · Misalkan a dan b adalah bilangan bulat dan m adalah bilangan > 0, maka $a \equiv b \pmod m$ jika m habis membagi a – b. · Jika a tidak kongruen dengan b dalam modulus m, maka ditulis $a \not\equiv b \pmod m$. Misalkan m adalah bilangan bulat positif. 1. Jika $a \equiv b \pmod m$ dan c adalah sembarang bilangan bulat maka (i) $(a + c) \equiv (b + c) \pmod m$ (ii) $ac \equiv bc \pmod m$ (iii) $a^p \equiv b^p \pmod m$ untuk suatu bilangan bulat tak negatif p. 2. Jika $a \equiv b \pmod m$ dan $c \equiv d \pmod m$, maka (i) $(a + c) \equiv (b + d) \pmod m$ (ii) $ac \equiv bd \pmod m$

2. Balikan Modulo (modulo invers)

Jika a dan m relatif prima dan m > 1, maka kita dapat menemukan balikan (invers) dari a modulo m. Balikan dari a modulo m adalah bilangan bulat a sedemikian sehingga $aa \equiv 1 \pmod m$

3. Kekongruenan Lanjar

Kekongruenan lanjar adalah kongruen yang berbentuk $ax \equiv b \pmod m$ dengan m adalah bilangan bulat positif, a dan b sembarang bilangan bulat, dan x adalah peubah bilangan bulat.

4. Chinese Remainder Problem

Pada abad pertama, seorang matematikawan China yang bernama Sun Tse mengajukan pertanyaan sebagai berikut: Tentukan sebuah bilangan bulat yang bila dibagi dengan 5 menyisakan 3, bila dibagi 7 menyisakan 5, dan bila dibagi 11 menyisakan 7. Pertanyaan Sun Tse dapat dirumuskan kedalam sistem kongruen lanjar: $x \equiv 3 \pmod 5$ $x \equiv 5 \pmod 7$ $x \equiv 7 \pmod{11}$. Misalkan m1, m2, …, mn adalah bilangan bulat positif sedemikian sehingga PBB(mi, mj) = 1 untuk $i \neq j$. Maka sistem kongruen lanjar $x \equiv ak \pmod{mk}$ mempunyai sebuah solusi unik modulo m = m1 × m2 × … × mn.

D. Aritmetika Modulo

Aritmetika modulo cocok digunakan untuk kriptografi karena dua alasan. Yang pertama, oleh karena nilai-nilai aritmetika modulo berada dalam himpunan berhingga (0 sampai modulus m – 1), maka kita tidak perlu khawatir hasil perhitungan berada di luar himpunan. Berikutnya karena kita bekerja dengan bilangan bulat, maka kita tidak khawatir kehilangan informasi akibat pembulatan (round off) sebagaimana pada operasi bilangan riil.

E. Kriptografi

Adalah ilmu dan seni untuk menjaga kerahasian pesan dengan cara menyandikannya ke dalam bentuk yang tidak dapat dimengerti lagi maknanya. Kata cryptography berasal dari bahasa Yunani: krupto (hidden atau secret) dan grafh (writing) Artinya “secret writing”

Informasi yang tidak bisa dimengerti maknanya itu dinamakan ciphertext. Sebaliknya informasi yang dapat dimengerti maknanya dinamakan plaintext. Plaintext dapat ditransformasikan menjadi ciphertext, begitu pula sebaliknya. Transformasi plaintext menjadi ciphertext dilakukan dengan menggunakan kriptografi.

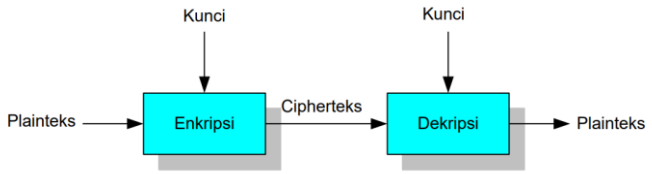
```
Ketika saya berjalan-jalan di pantai,
saya menemukan banyak sekali kepiting
yang merangkak menuju laut. Mereka
adalah anak-anak kepiting yang baru
menetas dari dalam pasir. Naluri
mereka mengatakan bahwa laut adalah
tempat kehidupan mereka.
```

Gambar 1 : Ilustrasi plaintext (Sumber: [2])

```
Ztâxzp/épêp/qtüyp{p}<yp{p}/sx/•p}âpx;
  épêp/|t}t|äzp}/qp}êpz/étzp{x/zt•xâx
}v  êp}v/|tüp}vzpz/|t}äyä/{päâ=/\tütz
p  psp{pw/p}pz<p}pz/zt•xâx}v/êp}
v/qpüä  |t}tâpé/spüx/sp{p|/•péxü=/]
p{äüx  |ttüzp/|t}vpâpzp}/qpwåp/{päâ
/psp{pw  ât|•pâ/ztwxsä•p}/|tützp=
```

Gambar 2 : Ilustrasi chipertext (Sumber: [2])

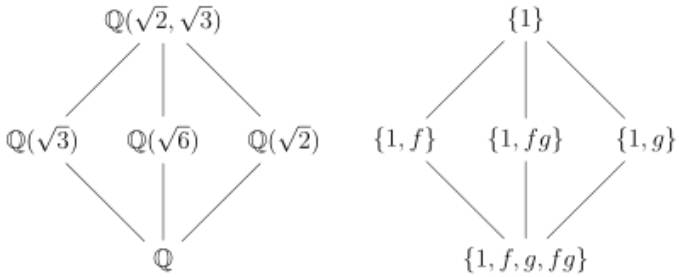
Kriptografi terdiri dari dua proses: 1. Enkripsi: transformasi dari plainteks menjadi cipherteks 2. Dekripsi: transformasi dari cipherteks menjadi plainteks



Gambar 3 : Ilustrasi proses enkripsi-dekripsi (Sumber: [2])

F. Galois

Teori Galois menyediakan hubungan antara teori medan dan teori grup. Konjektur menggunakan teori Galois, masalah-masalah tertentu dalam teori medan dapat direduksi menjadi teori grup, yang dalam arti tertentu lebih sederhana dan lebih dipahami. Ini telah digunakan untuk memecahkan masalah klasik termasuk menunjukkan bahwa dua masalah kuno tidak dapat diselesaikan seperti yang dinyatakan (menggandakan kubus dan melipatgandakan sudut); menunjukkan bahwa tidak ada rumus kuintik; dan menunjukkan poligon yang dapat dibangun.



Gambar 4 : Ilustrasi Diagram kisi dari **Q** berdampingan dengan akar kuadrat positif dari 2 dan 3, sub-bidangnya (Sumber: [3])

G. 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. 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:

$$y^2 = x^3 + ax + b$$

III. PEMBAHASAN

Langkah pertama dalam kriptografi kurva eliptik adalah menentukan titik-titik kurva eliptik. Misalkan kita memilih nilai p = 11. Selanjutnya, kita menentukan nilai a dan b sebagai bilangan bulat positif. Untuk contoh ini, kita pilih a = 3 dan b = 5. Dengan nilai-nilai tersebut, kita dapat menentukan persamaan kurva eliptik. Persamaan kurva eliptik pada umumnya memiliki bentuk

$$y^2 = x^3 + 3x + 5 \ (mod\ 17)$$

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

$$4a^3 + 27b^2 (mod\ p) \neq 0$$

$$4.3^3 + 27.5^2 (mod\ 11) \neq 0$$

$$4.3^3 + 27.5^2 (mod\ 11) = 108 + 675\ (mod\ 11)$$

$$4.3^3 + 27.5^2 (mod\ 11) = 783\ (mod\ 11) = 2 \neq 0$$

Maka diperoleh persamaan

$$y^2 = x^3 + 3x + 5 \ (mod\ 17)$$

Untuk dapat membuat titik (x, y) maka tentukan terlebih dahulu elemen dari kurva eliptik $E_{17}(4,7)$ atas GF_{11}, sebagai berikut: GF_{11} = {0,1,2,3,4,5,6,7,8,9,10}. Sebelum membentuk semua titik (x, y) tenukan terlebih dahulu daerah elemen/ range kurva eliptik QR_{11} (Quadratic Residue Module). Pada Tabel 1 berikut ini merupakan quadratic residue module dari GF_{11}

GFp	y^2 mod 11	QR_{11}
0	$0^2 (mod\ 11)$	0
1	$1^2 (mod\ 11)$	1
2	$2^2 (mod\ 11)$	4
3	$3^2 (mod\ 11)$	9

4	$4^2 (mod\ 11)$	5
5	$5^2 (mod\ 11)$	3
6	$6^2 (mod\ 11)$	3
7	$7^2 (mod\ 11)$	5
8	$8^2 (mod\ 11)$	9
9	$9^2 (mod\ 11)$	4
10	$10 (mod\ 11)$	1

Tabel 1 Quadratic Residue Modulo 11

Dari Tabel 1 di atas, diperoleh QR_{11} = {0,1,3,4,5,9}. Selanjutnya, akan ditentukan elemen grup kurva eliptik $E_{13}(3,5)$ yang merupakan himpunan penyelesaian dari $y^2 = x^3 + 3x + 5$ $(mod\ 11)$ untuk $x \in GF_{11}$ dan $y^2 \in QR_{11}$. Berikut ini dalam Tabel 2 diberikan elemen-elemen dari gurp kurva eliptik yang terbentuk dari kurva eliptik $y^2 = x^3 + 3x + 5$ atas lapangan Galois prima GF_{11}.

x	$y^2 = x^3 + 3x + 5\ (mod\ 11)$	$(x,y) \in E_{13}(3,5)$
0	$y^2 = 0^3 + 3.0 + 5\ (mod\ 11) = 0$	-
1	$y^2 = 1^3 + 3.1 + 5\ (mod\ 11) = 9$	(1,3) & (1,8)
2	$y^2 = 2^3 + 3.2 + 5\ (mod\ 11) = 8$	-
3	$y^2 = 3^3 + 3.3 + 5\ (mod\ 11) = 8$	-
4	$y^2 = 4^3 + 3.4 + 5\ (mod\ 11) = 4$	(4,2) & (4,9)
5	$y^2 = 5^3 + 3.5 + 5\ (mod\ 11) = 2$	-
6	$y^2 = 6^3 + 3.6 + 5\ (mod\ 11) = 8$	-
7	$y^2 = 7^3 + 3.7 + 5\ (mod\ 11) = 6$	-
8	$y^2 = 8^3 + 3.8 + 5\ (mod\ 11) = 2$	-
9	$y^2 = 9^3 + 3.9 + 5\ (mod\ 11) = 2$	-
10	$y^2 = 10^3 + 3.10 + 5\ (mod\ 11) = 1$	(10,1) & (10,10)

Tabel 2 Elemen Grup Kurva Eliptik

Oleh sebab itu diperoleh Grup Eliptik sebagai berikut: $E_{11}(3,5)$ = {(1,3), (1,8), (4,2), (4,9), (10,1), (10,10)}. Setelah itu, langkah selanjutnya adalah memilih salah satu titik yang akan dijadikan generator atau pembangkit G. Untuk merepresentasikan titik-titik kurva eliptik dalam konteks simbol bilangan, huruf, dan elemen lainnya, diperlukan penentuan pembangkit, yaitu G. Representasi ini sangat bergantung pada titik yang dipilih, sehingga tidak mungkin diterapkan secara umum.

Keunggulan kriptografi ini terletak pada jumlah titik yang ada pada suatu kurva, sulitnya untuk mengetahui bentuk kurva yang digunakan. Metode kriptografi kurva eliptik melibatkan dua kunci dalam proses enkripsi dan dekripsi, yaitu kunci publik dan kunci privat. Kunci publik adalah titik acak pada kurva, diperoleh melalui perkalian antara kunci privat dan titik pembangkit atau generator G. Sementara itu, kunci privat merupakan angka yang ditentukan sendiri.

Berikut ini disajikan contoh pembentukan kunci publik dan kunci privat untuk mengilustrasikan metode tersebut.

$E_{11}(3,5)$ = {(1,3), (1,8), (4,2), (4,9), (10,1), (10,10)}.

Langkah berikutnya adalah menentukan titik pembangkit atau generator $G \in E_{11}(3,5)$. Sebagai contoh, kita ambil G = (4,9). Setelah itu, kita menentukan kunci privat d secara acak dengan memastikan bahwa $d \in 2,3, \ldots\ p - 1 \in GFp$. Sebagai contoh, kita tentukan d = 2. Setelah menetapkan generator G = (4,9) dan kunci privat d = 2, langkah selanjutnya adalah menghitung kunci publik Q. Ini dilakukan dengan menggunakan persamaan penjumlahan titik pada kurva eliptik pada GFp antara nilai d dan titik G.

$Q = d\ .\ G$
$Q = 2\ .\ (4,9)$
$Q = (4,9) + (4,9)$
$Q = (8,18)$

Maka diperoleh nilai kunci publik $Q = (8,18)$.

Langkah awal proses enkripsi, yaitu menentukan titik pembangkit yang dalam penelitian ini memilih contoh G = (4,9) sebagai representasi huruf A. Huruf A dapat dituliskan sebagai θ, maka diperoleh $A = \theta$ = (4,9). Sedangkan huruf BB dapat dituliskan sebagai 2θ, sehingga diperoleh $B = 2\theta$ = (8,6). Nilai 2θ dapat dicari dengan menggunakan operasi penggandaan titik-titik kurva eliptik. Untuk huruf, angka dan symbol yang lainnya dapat direpresentasikan menjadi 3θ, 4θ, … n dengan menggunakan operasi penjumlahan atau penggandaan titik kurva eliptik. Langkah selanjutnya, yaitu memilih suatu bilangan acak $k \in [\ 1, n - 1\ ]$. Dipilih k = 2.

Menghitung nilai (C_1 , C_2) yang merupakan ciphertext, dengan $C_1 = k.\ G$. karena nilai $C1$ sama untuk setiap representasi symbol menjadi titik –titik kurva eliptik, maka cukup dihitung satu kali. Diketahui nilai k = 4 dan nilai G = (4,9), maka dengan menggunakan operasi penjumlahan dan penggandaan titik-tiitk kurva eliptik diperoleh:

$C_1 = \mathrm{k}\ .\ G$
$C_1 = 2\ .\ (4,9)$
$C_1 = (4,9) + (4,9)$
$C_1 = (6,5)$

Menghitung nilai C_2 menggunakan rumus $C_2 = M + k.Q$. M merupakan plaintext yang sudah dikonversikan ke dalam titik-titik kurva eliptik, Q = (8,18) merupakan kunci publik dan k = 2 dengan menggunakan operasi penggandaan dan penjumlahan titik-titik kurva eliptik.

Untuk C_2 A, diperoleh:
$C_1 = M + k.Q$
$C_1 = (4,9) + ((8,18) + (8,18))$
$C_1 = (4,9) + (6,4)$
$C_1 = (3,6)$

Untuk C_2 B, diperoleh:
$C_1 = M + k.Q$
$C_1 = (8,6) + ((8,18) + (8,18))$
$C_1 = (8,6) + (6,4)$
$C_1 = (9,4)$

Diperoleh ciphertext untuk huruf $A = (C_1, C_2) = ((6,5), (3,6))$ dan ciphertext untuk huruf $B = (C_1, C_2) = ((6,5), (9,4))$.

Supaya pesan dapat terbaca, maka perlu dilakukan proses dekripsi. Berikut langkah-langkah dekripsi pesan:

Menghitung nilai pesan teks $M = C_2 - d.\ C_1$, dengan kunci privat $d = 2$

Untuk A, diperoleh:
$M = C_2 - d.\ C_1$
$M = (3,6) - 2.(6,5)$
$M = (3,6) - (10,6)$
$M = (4,9)$

Untuk B, diperoleh:
$M = C_2 - d.\ C_1$
$M = (9,4) - 2.(6,5)$
$M = (9,4) - (10,6)$
$M = (8,6)$

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 dengan Python diharapkan dapat meningkatkan keamanan sistem dengan menggunakan nilai yang lebih besar dan mempercepat proses penentuan titik-titik kurva eliptik, proses enkripsi dan proses dekripsi pada algoritma kriptografi. Diambil contoh nilai $a = 21$, $b = 34$ dan $p = 317$. Berikut tampilan awal GUI Python dapat dilihat pada Gambar 3 di bawah ini:

Titik kurva	Simbol	Titik kurva	Simbol
3,21	A	311,314	T
60,95	B	151,7	U
223,66	C	200,139	V
140,304	D	142,47	W
9,316	E	209,148	X
248,32	F	121,134	Y
302,214	G	44,66	Z
216,308	H	301,255	0
105,230	I	220,249	1
288,37	J	50,251	2
161,236	K	46,180	3
242,41	L	108,210	4
11,168	M	298,82	5
180,174	N	230,277	6
176,39	O	127,219	7
34,181	P	12,72	8
304,307	Q	158,263	9
67,172	R	20,294	+
7,29	S	89,127	?

Tabel 3 Representasi titik kurva

Gambar 5 Tampilan Fitur Penggandaan Titik

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":

Karakater	C_1	C_2
M	248,32	73,255
A	248,32	6,196
T	248,32	297,217
E	248,32	79,264
M	248,32	73,255
A	248,32	6,196
T	248,32	297,217
I	248,32	177,220
K	248,32	16,36
A	248,32	6,196

Tabel 4 Enkripsi "MATEMATIKA"

Selanjutnya, untuk hasil dari proses dekripsi dapat dilihat pada Tabel 5 di bawah ini (d = 7)

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

Tabel 5 Dekripsi chiper

IV. KESIMPULAN

Berdasarkan hasil penelitian ini, dapat disarikan bahwa implementasi Kriptografi Kurva Eliptik di dalam Galois field prima mengandalkan konsep matematika. Sistem kriptografi ini terbukti efektif untuk menjaga kerahasiaan pesan atau informasi, terutama karena perhitungan titik-titik kurva eliptik yang kompleks membuat retas keamanannya menjadi sangat sulit.

Implementasi Kriptografi Kurva Eliptik menggunakan Python terdiri dari tiga tahap utama, yaitu pembentukan kunci, enkripsi, dan dekripsi. Proses pembentukan kunci menghasilkan kunci publik dan kunci rahasia. Pada tahap enkripsi, plaintext diambil sebagai input dan dienkripsi menggunakan kunci publik dan kunci privat, menghasilkan ciphertext. Sebaliknya, tahap dekripsi menerima input berupa ciphertext dan kunci privat, dan menghasilkan plaintext.

Penelitian ini menunjukkan bahwa implementasi menggunakan Python memberikan keuntungan tambahan dalam percepatan proses perhitungan sistem Kriptografi Kurva Eliptik pada Galois field prima. Hal ini menandakan potensi efisiensi yang dapat diperoleh dengan memanfaatkan bahasa pemrograman Python dalam konteks ini.

REFERENSI

[1] Rinaldi Munir, "Teori Bilangan (Number Theory)", https://informatika.stei.itb.ac.id/~rinaldi.munir/Kriptografi/Teori%20Bilangan.pdf, diakses, 8 Desember 2023 pukul 22.32 .

[2] Rinaldi Munir, "Pengenalan Kriptografi dan Steganografi untuk Keamanan Informasi", https://jatinangor.itb.ac.id/wp-content/uploads/sites/17/2016/10/Pengenalan-Kriptografi-Untuk-Keamanan-Informasi.pdf, diakses, 8 Desember 2023 pukul 23.46 .

[3] https://p2k.stekom.ac.id/ensiklopedia/Teori_Galois, diakses, 9 Desember 00.43 .

[4] J. Wang, "Fundamentals of erbium-doped fiber amplifiers arrays (Periodical style—Submitted for publication)," *IEEE J. Quantum Electron.*, submitted for publication.

[5] C. J. Kaufman, Rocky Mountain Research Lab., Boulder, CO, private communication, May 1995.

V. UCAPAN TERIMA KASIH

Puji syukur penulis panjatkan kepada Tuhan Yang Maha Esa yang telah memberikan karunia, sehingga penulis dapat Makalah IF2120 Matematika Diskrit – Sem. I Tahun 2023/2024 menyelesaikan makalah yang berjudul "Analisis Kombinatorial Pada Pengkodean dan Dekode Galois" yang selesai tepat pada waktunya. Tak lupa juga penulis mengucapkan terima kasih kepada Ibu Fariska Zakhralativa Ruskanda, S.T., M.T. sebagai dosen pengampu mata kuliah IF2120 Matematika Diskrit Kelas 02 atas bimbingan dan pengajaran yang telah dilakukan di kelas Matematika Diskrit ini. Penulis juga mengucapkan terima kasih kepada Bapak Dr. Ir. Rinaldi Munir, MT. sebagai salah satu dosen pengampu Matematika Diskrit yang memberikan referensi dan sumber pembelajaran Matematika Diskrit melalui situs beliau. Terakhir, penulis mengucapkan terima kasih kepada orang tua, keluarga, dan seluruh pihak yang membantu penulis dalam menyelesaikan makalah ini

PERNYATAAN

Dengan ini saya menyatakan bahwa makalah yang saya tulis ini adalah tulisan saya sendiri, bukan saduran, atau terjemahan dari makalah orang lain, dan bukan plagiasi.

Bandung, 9 Desember 2023

Dimas Bagoes Hendrianto
13522112