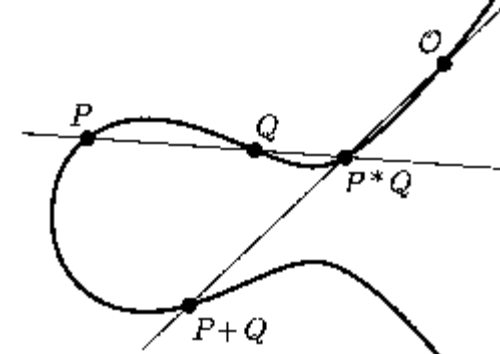


II4031 Kriptografi dan Koding



# Elliptic Curve Cryptography (ECC)

(Bagian 1)



Oleh: Rinaldi Munir

Program Studi Sistem dan Teknologi Informasi  
Sekolah Teknik Elektro dan Informatika

## Referensi:

1. Andreas Steffen, *Elliptic Curve Cryptography*, Zürcher Hochschule Winterthur.
2. Debdeep Mukhopadhyay, *Elliptic Curve Cryptography* , Dept of Computer Sc and Engg IIT Madras.
3. Anoop MS , *Elliptic Curve Cryptography, an Implementation Guide*

# Pengantar

- Sebagian besar kriptografi kunci-publik ( seperti RSA, ElGamal, Diffie-Hellman) menggunakan bilangan bulat yang sangat besar dalam komputasinya.
- Sistem seperti itu memiliki masalah yang signifikan dalam menyimpan, memproses kunci dan pesan, dan membutuhkan waktu komputasi yang lama.
- Sebagai alternatif adalah melakukan komputasi berbasis kurva eliptik (*elliptic curve*).
- Kriptografi yang menggunakan kurva eliptik dinamakan *Elliptic Curve Cryptography* (ECC).
- Komputasi dengan kurva eliptik menawarkan keamanan yang sama dengan algoritma-algoritma tersebut namun dengan ukuran kunci yang lebih kecil.

Sumber: William Stallings, *Cryptography and Network Security*

- ECC adalah kriptografi kunci-publik yang relatif lebih baru usianya.
- Dikembangkan oleh Neal Koblitz dan Victor S. Miller tahun 1985.
- Klaim: Panjang kunci ECC lebih pendek daripada kunci RSA, namun memiliki tingkat keamanan yang sama dengan RSA.
- Contoh: kunci ECC sepanjang 160-bit menyediakan keamanan yang sama dengan 1024-bit kunci RSA.
- Keuntungan: dengan panjang kunci yang lebih pendek, membutuhkan memori dan komputasi yang lebih sedikit.
- Cocok untuk piranti nirkabel, dimana prosesor, memori, umur batere terbatas.

# Teori Aljabar Abstrak

- Sebelum membahas ECC, perlu dipahami konsep aljabar abstrak yang mendasarinya.
- Konsep aljabar abstrak:
  1. Grup (*group*)
  2. Medan (*field*)

# Grup

- Grup (*group*) adalah sistem aljabar yang terdiri dari:
  - sebuah himpunan  $G$
  - sebuah operasi biner  $*$

sedemikian sehingga untuk semua elemen  $a$ ,  $b$ , dan  $c$  di dalam  $G$  berlaku aksioma berikut:

1. *Closure*:  $a * b$  harus berada di dalam  $G$
  2. Asosiatif:  $a * (b * c) = (a * b) * c$
  3. Elemen netral: terdapat  $e \in G$  sedemikian sehingga  $a * e = e * a = a$
  4. Elemen invers: terdapat  $a' \in G$  sedemikian sehingga  $a * a' = a' * a = e$
- Notasi:  $\langle G, * \rangle$

- $\langle G, + \rangle$  menyatakan sebuah grup dengan operasi penjumlahan.
- $\langle G, \cdot \rangle$  menyatakan sebuah grup dengan operasi perkalian

Contoh-contoh grup:

1.  $\langle \mathbb{R}, + \rangle$  : grup dengan himpunan bilangan riil dengan operasi +  
 $e = 0$  dan  $a' = -a$
2.  $\langle \mathbb{R}^*, \cdot \rangle$  : grup dengan himpunan bilangan riil tidak nol (yaitu,  $\mathbb{R}^* = \mathbb{R} - \{0\}$ )  
dengan operasi kali ( $\cdot$ )  
 $e = 1$  dan  $a' = 1/a = a^{-1}$
3.  $\langle \mathbb{Z}, + \rangle$  dan  $\langle \mathbb{Z}, \cdot \rangle$  masing-masing adalah grup dengan himpunan bilangan bulat (*integer*) dengan operasi + dan  $\cdot$ .

4.  $\langle \mathbb{Z}_n, \oplus \rangle$  : grup dengan himpunan *integer* modulo  $n$ , yaitu  $\mathbb{Z}_n = \{0, 1, 2, \dots, n - 1\}$  dan  $\oplus$  adalah operasi penjumlahan modulo  $n$ .

Contoh:  $n = 5$ ,  $\mathbb{Z}_n = \{0, 1, 2, 3, 4\}$ ,  $(3 \oplus 4) = (3 + 4) \bmod 5 = 2$

$\langle \mathbb{Z}_p, \oplus \rangle$  : grup dengan himpunan *integer* modulo  $p$ ,  $p$  adalah bilangan prima, yaitu  $\mathbb{Z}_p = \{0, 1, 2, \dots, p - 1\}$  dan  $\oplus$  adalah operasi penjumlahan modulo  $p$ .

$\langle \mathbb{Z}_p^*, \otimes \rangle$  : dengan himpunan integer bukan nol,  $p$  adalah bilangan prima, yaitu  $\mathbb{Z}_p^* = \{1, 2, \dots, p - 1\}$  dan  $\otimes$  adalah operasi perkalian modulo  $p$ .



- Sebuah grup  $\langle G, * \rangle$  dikatakan **grup komutatif** atau **grup abelian** (atau disingkat **abelian** saja) jika berlaku aksioma komutatif  $a * b = b * a$  untuk semua  $a, b \in G$ .
- $\langle \mathbb{R}, + \rangle$  dan  $\langle \mathbb{R}, \cdot \rangle$  adalah abelian
- $\langle \mathbb{Z}, + \rangle$  dan  $\langle \mathbb{Z}, \cdot \rangle$  adalah abelian
- tetapi,  $\langle M, \times \rangle$ , dengan  $M$  adalah himpunan matriks  $2 \times 2$  dengan determinan  $\neq 0$  bukan abelian (tanya kenapa?)

Ket: Abelian diambil dari kata “abel”, untuk menghormati Niels Abel, seorang Matematikawan Norwegia (1802 – 1829)

**Niels Henrik Abel** (5 August 1802 – 6 April 1829) was a [Norwegian mathematician](#) who made pioneering contributions in a variety of fields. His most famous single result is the first complete proof demonstrating the impossibility of solving the [general quintic equation](#) in radicals. This question was one of the outstanding open problems of his day, and had been unresolved for 250 years. He was also an innovator in the field of [elliptic functions](#), discoverer of [Abelian functions](#). Despite his achievements, Abel was largely unrecognized during his lifetime; he made his discoveries while living in poverty and died at the age of 26.

Most of his work was done in six or seven years of his working life.<sup>[1]</sup> Regarding Abel, the French mathematician [Charles Hermite](#) said: "Abel has left mathematicians enough to keep them busy for five hundred years."<sup>[1][2]</sup> Another French mathematician, [Adrien-Marie Legendre](#), said: "*quelle tête celle du jeune Norvégien!*" ("what a head the young Norwegian has!").<sup>[3]</sup>

Sumber: Wikipedia

Born	5 August 1802 <a href="#">Nedstrand, Norway</a>
Died	6 April 1829 (aged 26) <a href="#">Froland, Norway</a>
Residence	Norway
Nationality	Norwegian
Fields	<a href="#">Mathematics</a>
<i>Alma mater</i>	<a href="#">Royal Frederick University</a>
Known for	



[Abel's binomial theorem](#)  
[Abelian category](#)  
[Abelian variety](#)  
[Abelian variety of CM-type](#)  
[Abel equation](#)  
[Abel equation of the first kind](#)  
[Abelian extension](#)  
[Abel function](#)  
[Abelian group](#)  
[Abel's identity](#)  
[Abel's inequality](#)  
[Abel's irreducibility theorem](#)  
[Abel–Jacobi map](#)  
[Abel–Plana formula](#)  
[Abel–Ruffini theorem](#)  
[Abelian means](#)  
[Abel's summation formula](#)  
[Abel's theorem](#)  
[Abel transform](#)  
[Abel transformation](#)  
[Abelian variety](#)  
[Dual abelian variety](#)

# Medan (*Field*)

- Medan (*field*) adalah himpunan elemen (disimbolkan dengan  $F$ ) dengan dua operasi biner, biasanya disebut penjumlahan ( $+$ ) dan perkalian ( $\cdot$ ).
- Sebuah struktur aljabar  $\langle F, +, \cdot \rangle$  disebut medan jika dan hanya jika:
  1.  $\langle F, + \rangle$  adalah grup abelian
  2.  $\langle F - \{0\}, \cdot \rangle$  adalah grup abelian
  3. Operasi  $\cdot$  menyebar terhadap operasi  $+$  (sifat distributif)  
Distributif:  $x \cdot (y + z) = (x \cdot y) + (x \cdot z)$   
 $(x + y) \cdot z = (x \cdot z) + (y \cdot z)$
- Jadi, sebuah medan memenuhi aksioma: *closure*, komutatif, asosiatif, dan distributif

- Contoh medan:
  - medan bilangan bulat,  $\langle \mathbb{Z}, +, \cdot \rangle$
  - medan bilangan riil,  $\langle \mathbb{R}, +, \cdot \rangle$
  - medan bilangan rasional ( $p/q$ )  $\langle \mathbb{Q}, +, \cdot \rangle$
- Sebuah medan disebut berhingga (*finite field*) jika himpunannya memiliki jumlah elemen yang berhingga.  
Jika jumlah elemen himpunan adalah  $n$ , maka notasinya  $F_n$   
Contoh:  $F_2$  adalah medan dengan elemen 0 dan 1
- Medan berhingga sering dinamakan juga **Galois Field**, untuk menghormati Evariste Galois, seorang matematikawan Perancis (1811 – 1832)

## Evariste Galois



Born	25 October 1811 <a href="#">Bourg-la-Reine, French Empire</a>
Died	31 May 1832 (aged 20) Paris, <a href="#">Kingdom of France</a>
Nationality	French
Fields	Mathematics
Known for	Work on the <a href="#">theory of equations</a> and <a href="#">Abelian integrals</a>

# Medan Berhingga $F_p$

- Kelas medan berhingga yang penting adalah  $F_p$
- $F_p$  adalah medan berhingga dengan himpunan bilangan bulat  $\{0, 1, 2, \dots, p-1\}$  dengan  $p$  bilangan prima, dan dua operasi yang didefinisikan sbb:

## 1. Penjumlahan

Jika  $a, b \in F_p$ , maka  $a + b = r$ , yang dalam hal ini  
 $r = (a + b) \bmod p, 0 \leq r \leq p - 1$

## 2. Perkalian

Jika  $a, b \in F_p$ , maka  $a \cdot b = s$ , yang dalam hal ini  
 $s = (a \cdot b) \bmod p, 0 \leq s \leq p - 1$

**Contoh:**  $F_{23}$  mempunyai anggota  $\{0, 1, 2, \dots, 22\}$ .

Contoh operasi aritmetika:

$$12 + 20 = 9 \text{ (karena } 12 + 20 = 32 \text{ mod } 23 = 9)$$

$$8 \cdot 9 = 3 \text{ (karena } 8 \times 9 = 72 \text{ mod } 23 = 3)$$

# Medan Galois (*Galois Field*)

- Medan Galois adalah medan berhingga dengan  $p^n$  elemen,  $p$  adalah bilangan prima dan  $n \geq 1$ .
- Notasi:  $GF(p^n)$
- Kasus paling sederhana: bila  $n = 1 \rightarrow GF(p)$ , yang dalam hal ini elemen-elemennya dinyatakan di dalam himpunan  $\{0, 1, 2, \dots, p - 1\}$  dan operasi penjumlahan dan perkalian dilakukan dalam modulus  $p$ .



$p = 2 \rightarrow$

$GF(2):$

+	0	1
0	0	1
1	1	0

.	0	1
0	0	0
1	0	1

$p = 3 \rightarrow$

$GF(3):$

+	0	1	2
0	0	1	2
1	1	2	0
2	2	0	1

.	0	1	2
0	0	0	0
1	0	1	2
2	0	2	1

- Contoh: Bentuklah tabel perkalian untuk GF(11), kemudian tentukan solusi untuk  $x^2 \equiv 5 \pmod{11}$

.	0	1	2	3	4	5	6	7	8	9	10
0	0	0	0	0	0	0	0	0	0	0	0
1	0	1	2	3	4	5	6	7	8	9	10
2	0	2	4	6	8	10	1	3	5	7	9
3	0	3	6	9	1	4	7	10	2	5	8
4	0	4	8	1	5	9	2	6	10	4	7
5	0	5	10	4	9	3	8	2	7	1	6
6	0	6	1	7	2	8	3	9	4	10	5
7	0	7	3	10	6	2	9	5	1	8	4
8	0	8	5	2	10	7	4	1	9	6	3
9	0	9	7	5	3	1	10	8	6	4	2
10	0	10	9	8	7	6	5	4	3	2	1

$$x^2 \equiv 5 \pmod{11}$$

Maka:

$$x^2 = 16 \rightarrow x_1 = 4$$

$$x^2 = 49 \rightarrow x_2 = 7$$

Cara lain: cari elemen diagonal = 5, lalu ambil elemen mendatar atau elemen Vertikalnya (dilingkari).

Sumber: Andreas Steffen, Elliptic Curve Cryptography

# Galois Field $GF(2^m)$

- Disebut juga medan berhingga biner.
- $GF(2^m)$  atau  $F_2^m$  adalah ruang vektor berdimensi  $m$  pada  $GF(2)$ . Setiap elemen di dalam  $GF(2^m)$  adalah integer dalam representasi biner sepanjang maksimal  $m$  bit.
- String biner  $a_{m-1}a_{m-2} \dots a_1a_0$ ,  $a_i \in \{0,1\}$ , dapat dinyatakan dalam polinom  $a_{m-1}x^{m-1} + a_{m-2}x^{m-2} + \dots + a_1x + a_0$
- Jadi, setiap  $a \in GF(2^m)$  dapat dinyatakan sebagai
$$a = a_{m-1}x^{m-1} + a_{m-2}x^{m-2} + \dots + a_1x + a_0$$
- Contoh:  $m = 4 \rightarrow a = 1101$  dapat dinyatakan dengan  $x^3 + x^2 + 1$

## Operasi aritmetika pada $GF(2^m)$

Misalkan  $a = (a_{m-1} \dots a_1 a_0)$  dan  $b = (b_{m-1} \dots b_1 b_0) \in GF(2^m)$

- **Penjumlahan:**

$a + b = c = (c_{m-1} \dots c_1 c_0)$ , yang dalam hal ini  $c_i = (a_i + b_i) \bmod 2$ ,  $c \in GF(2^m)$

- **Perkalian:**  $a \cdot b = c = (c_{m-1} \dots c_1 c_0)$ , yang dalam hal ini  $c$  adalah sisa pembagian polinom  $a(x) \cdot b(x)$  dengan *irreducible polynomial* derajat  $m$ ,  $c \in GF(2^m)$

**Contoh:** Misalkan  $a = 1101 = x^3 + x^2 + 1$  dan  $b = 0110 = x^2 + x$   
 $a$  dan  $b \in GF(2^4)$

$$(i) \quad a + b = (x^3 + x^2 + 1) + (x^2 + x) = x^3 + 2x^2 + x + 1 \pmod{2}$$

Bagi tiap koefisien dengan 2,  
lalu ambil sisanya

$$= x^3 + 0x^2 + x + 1$$
$$= x^3 + x + 1$$

Dalam representasi biner:

1101

0110 +

1011 → sama dengan hasil operasi XOR

$$\therefore a + b = 1011 = a \text{ XOR } b$$

$$(ii) \quad a \cdot b = (x^3 + x^2 + 1) \cdot (x^2 + x) = x^5 + 2x^4 + x^3 + x^2 + x \pmod{2}$$

$$= x^5 + x^3 + x^2 + x = 10110$$

Karena  $m = 4$  hasilnya direduksi menjadi derajat  $< 4$  oleh sebuah *irreducible polynomial*  $f(x) = x^4 + x + 1$

Proses pembagiannya ditunjukkan sebagai berikut:

$$x^4 + x + 1 \overline{) \begin{array}{r} x \\ x^5 + x^3 + x^2 + x \\ \underline{x^5 + \quad \quad x^2 + x} \quad - \\ x^3 \end{array} \rightarrow \text{sisa pembagian}$$

Jadi,  $(x^5 + x^3 + x^2 + x) \pmod{f(x)} = x^3 = 1000$

$\therefore a \cdot b = 1000$

**Note:** Sebuah polinom dikatakan tidak dapat direduksi (*irreducible*) jika ia tidak dapat dinyatakan sebagai perkalian dari dua buah polinom lain (kecuali 1 dan dirinya sendiri).

Polinom  $x^2 + 1$  dan  $x^4 + x + 1$  adalah *irreducible* di dalam  $GF(2^n)$ , tetapi polinom  $x^5 + x^2 + x + 1$  *reducible* karena

$$x^5 + x^2 + x + 1 = (x^5 + x^2 + 1) \cdot (x^2 + 1)$$

# BERSAMBUNG