

Elliptic Curve Cryptography (ECC)

Oleh: Dr. Rinaldi Munir

Program Studi Informatika
Sekolah Teknik Elektro dan Informatika(STEI)
ITB

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 *integer* dengan bilangan yang sangat besar.
- Sistem seperti itu memiliki masalah yang signifikan dalam menyimpan dan memproses kunci dan pesan.
- Sebagai alternatif adalah menggunakan kurva eliptik (*elliptic curve*).
- Komputasi dengan kurva eliptik menawarkan keamanan yang sama dengan ukuran kunci yang lebih kecil.
- Kriptografi yang menggunakan kurva eliptik dinamakan *Elliptic Curve Cryptography* (ECC).

Sumber: William Stallings, *Cryptography and Network Security*
Chapter 10, 5th Edition

- ECC adalah algoritma kriptografi kunci publik yang lebih baru (meskipun belum dianalisis dengan baik).
- 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 .

$\langle \mathbb{Z}_p, \oplus \rangle$: 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 2×2 dengan determinan $\neq 0$ (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.^[1] Regarding Abel, the French mathematician [Charles Hermite](#) said: "Abel has left mathematicians enough to keep them busy for five hundred years."^{[1][2]}

Another French mathematician, [Adrien-Marie Legendre](#), said: "*quelle tête celle du jeune Norvégien!*" ("what a head the young Norwegian has!").^[3]

Sumber: Wikipedia

Born	5 August 1802 Nedstrand, Norway
Died	6 April 1829 (aged 26) Froland, Norway
Residence	Norway
Nationality	Norwegian
Fields	Mathematics
Alma mater	Royal Frederick University
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
 - medan bilangan riil
 - medan bilangan rasional (p/q)
- 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 Bourg-la-Reine, French Empire
Died	31 May 1832 (aged 20) Paris, Kingdom of France
Nationality	French
Fields	Mathematics
Known for	Work on the theory of equations and Abelian integrals

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 $n = 1 \rightarrow GF(p)$ dimana elemennya dinyatakan di dalam himpunan $\{0, 1, 2, \dots, p - 1\}$ dan operasi penjumlahan dan perkalian dilakukan dalam modulus p .

GF(2):

+	0	1
0	0	1
1	1	0

.	0	1
0	0	0
1	0	1

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). 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 $\alpha_{m-1} \dots \alpha_1 \alpha_0$, $\alpha_i \in \{0,1\}$, dapat dinyatakan dalam polinom $\alpha_{m-1}x^{m-1} + \dots + \alpha_1x + \alpha_0$
- Jadi, setiap $a \in GF(2^m)$ dapat dinyatakan sebagai
$$a = \alpha_{m-1}x^{m-1} + \dots + \alpha_1x + \alpha_0$$
- Contoh: 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:**

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

- **Perkalian:** $a \cdot b = c = (c_{m-1} \dots c_1 c_0)$ dimana 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) $a + b = (x^3 + x^2 + 1) + (x^2 + x) = x^3 + 2x^2 + x + 1 \pmod{2}$
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

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

$$\begin{aligned}
 \text{(ii) } a \cdot b &= (x^3 + x^2 + 1) \cdot (x^2 + x) = x^5 + 2x^4 + x^3 + x^2 + x \pmod{2} \\
 &= x^5 + x^3 + x^2 + x
 \end{aligned}$$

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

$$\begin{aligned}
 x^5 + x^3 + x^2 + x \pmod{f(x)} &= (x^4 + x + 1)x + x^5 + x^3 + x^2 + x \\
 &= 2x^5 + x^3 + 2x^2 + 2x \pmod{2} \\
 &= x^3
 \end{aligned}$$

$$\therefore a \cdot b = 1000$$

Kurva Eliptik

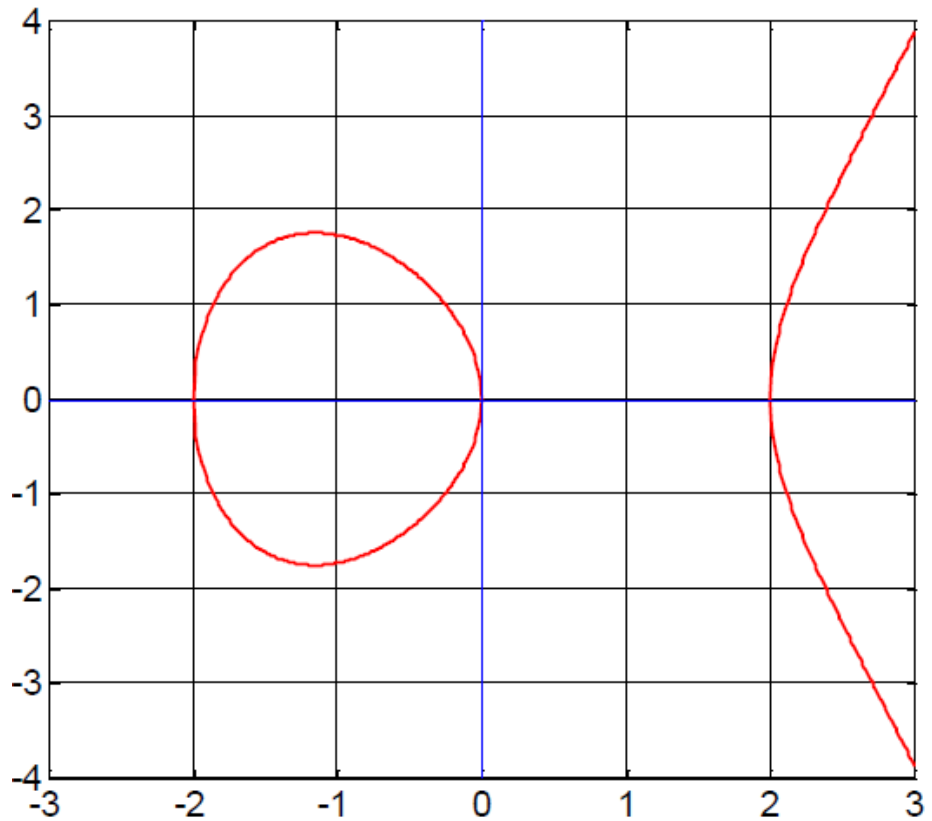
- Kurva eliptik adalah kurva dengan bentuk umum persamaan:

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

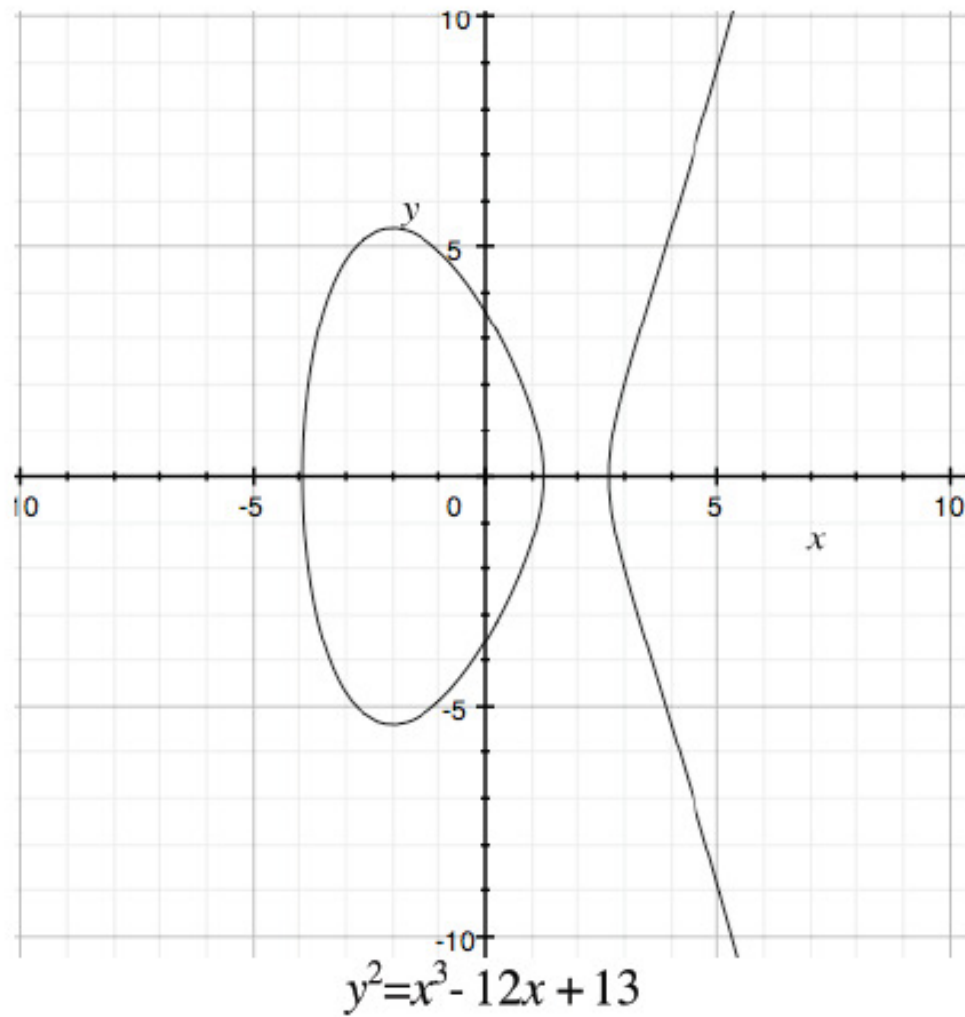
dengan syarat $4a^3 + 27b^2 \neq 0$

- Tiap nilai a dan b berbeda memberikan kurva eliptik yang berbeda.

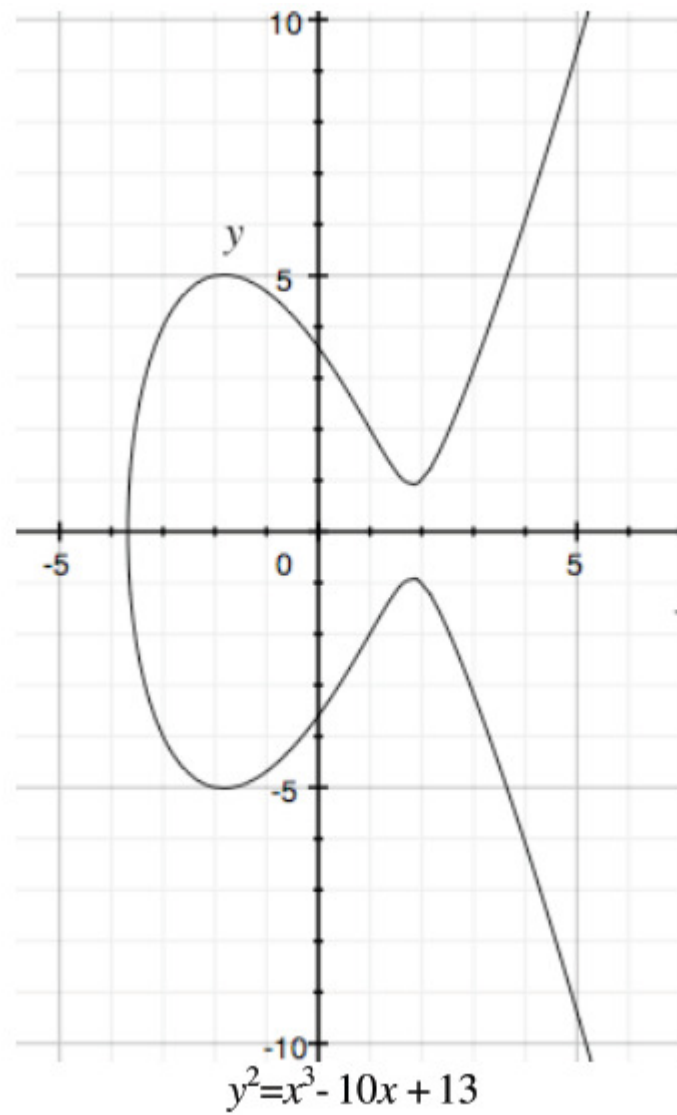
- Contoh: $y^2 = x^3 - 4x$
 $= x(x - 2)(x + 2)$



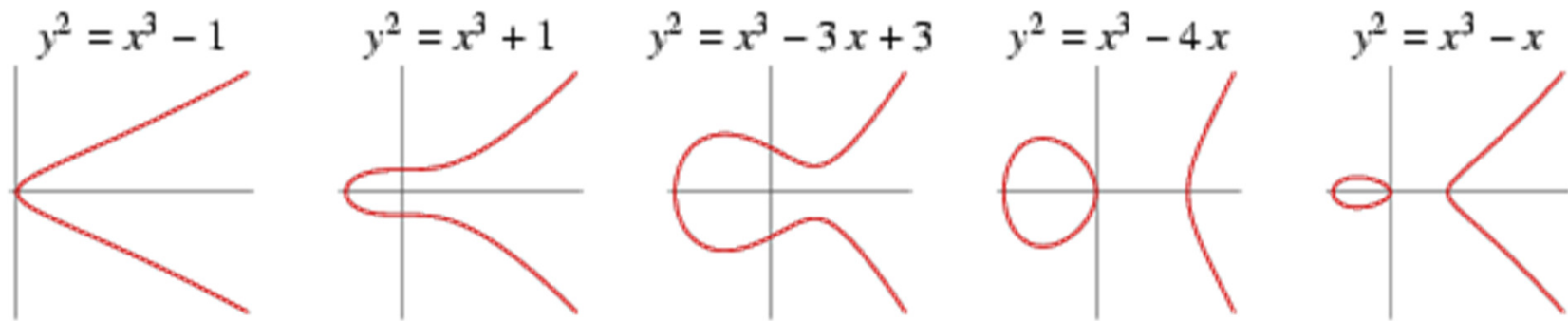
Sumber gambar: Andreas Steffen, Elliptic Curve Cryptography



Sumber gambar: Kevin Tirtawinata, Studi dan Analisis Elliptic Curve Cryptography



Sumber gambar: Kevin Tirtawinata, Studi dan Analisis Elliptic Curve Cryptography



Sumber gambar: **Debdeep Mukhopadhyay, Elliptic Curve Cryptography**,
 Dept of Computer Sc and Engg IIT Madras

- Kurva eliptik terdefinisi untuk $x, y \in \mathbb{R}$
- Didefinisikan sebuah titik bernama titik $O(x, \infty)$, yaitu titik pada *infinity*.
- Titik-titik $P(x, y)$ pada kurva eliptik bersama operasi $+$ membentuk sebuah grup.
 - Himpunan grup: semua titik $P(x, y)$ pada kurva eliptik
 - Operasi biner : $+$
- Penjelasan kenapa kurva eliptik membentuk sebuah grup dijelaskan pada *slide-slide* berikut ini.

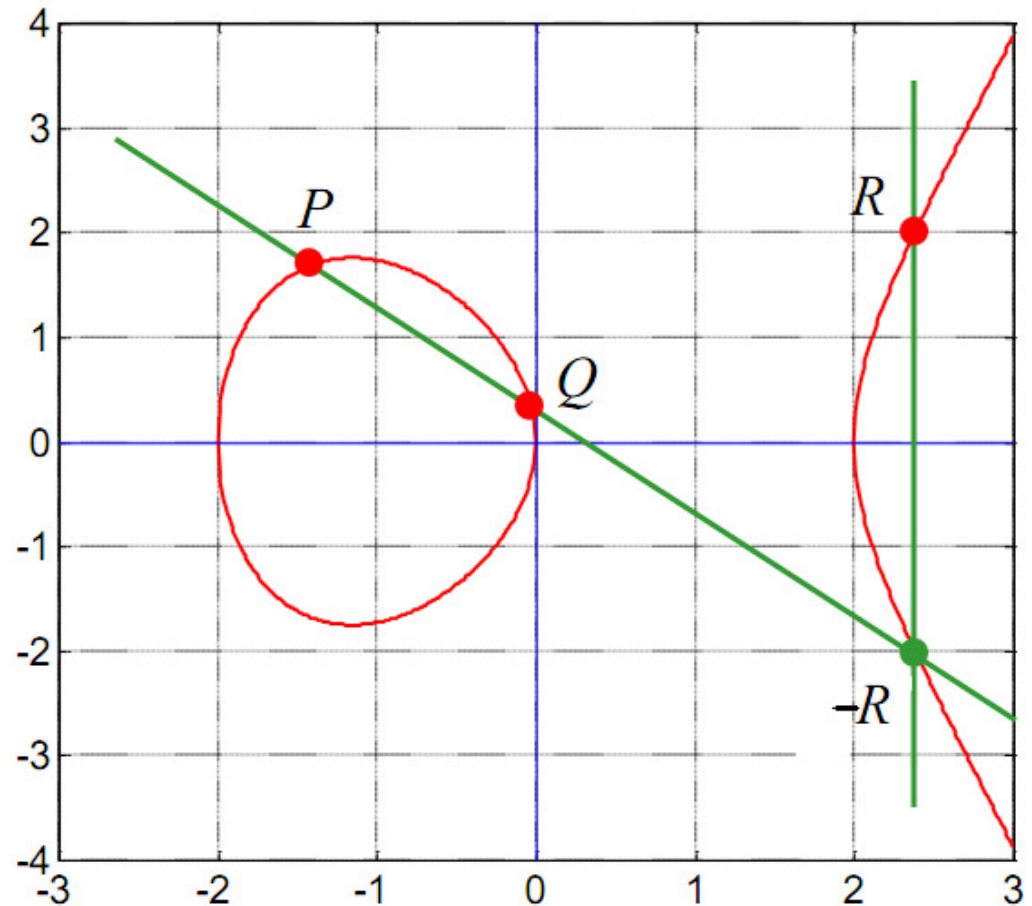
Penjumlahan Titik pada Kurva Eliptik

(a) $P + Q = R$

Penjelasan geometri:

1. Tarik garis melalui P dan Q
2. Jika $P \neq Q$, garis tersebut memotong kurva pada titik $-R$
3. Pencerminan titik $-R$ terhadap sumbu-x adalah titik R
4. Titik R adalah hasil penjumlahan titik P dan Q

Keterangan: Jika $R = (x, y)$ maka $-R$ adalah titik $(x, -y)$



Sumber gambar: Andreas Steffen, Elliptic Curve Cryptography

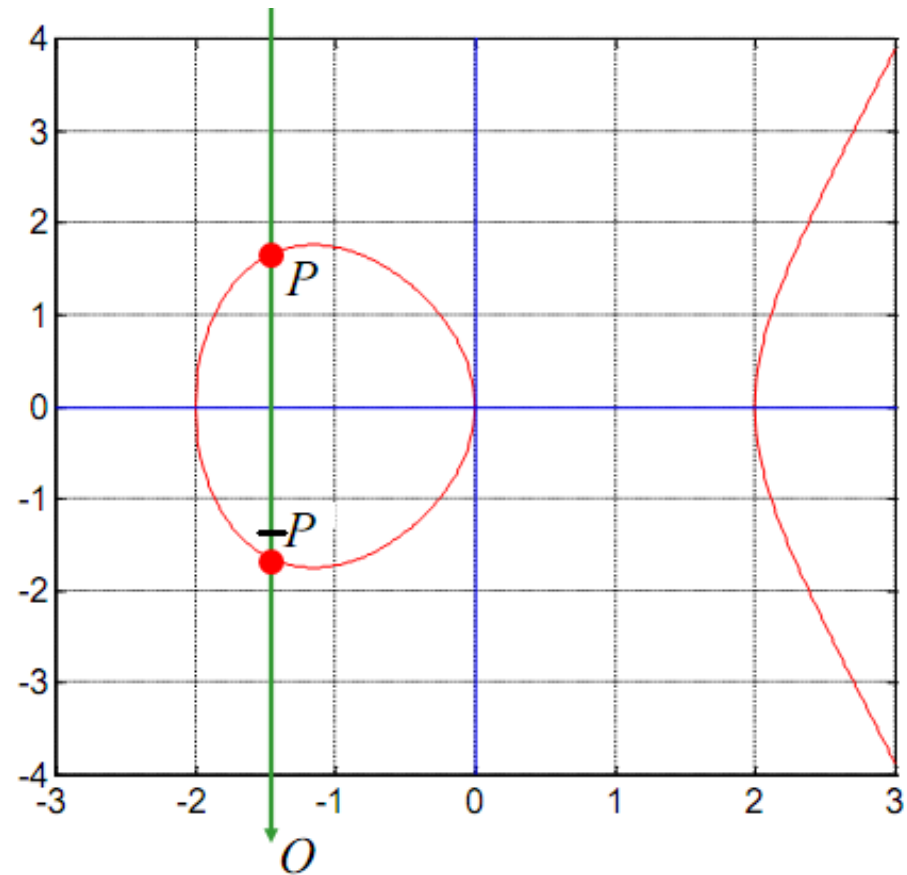
(b) $P + (-P) = O$, di sini O adalah titik di *infinity*

$P' = -P$ adalah elemen invers:

$$P + P' = P + (-P) = O$$

O adalah elemen netral:

$$P + O = O + P = P$$



Sumber gambar: Andreas Steffen, Elliptic Curve Cryptography

Penjelasan Analitik

Persamaan garis g : $y = \lambda x + \beta$

Gradien garis g : $\lambda = \frac{y_p - y_q}{x_p - x_q}$

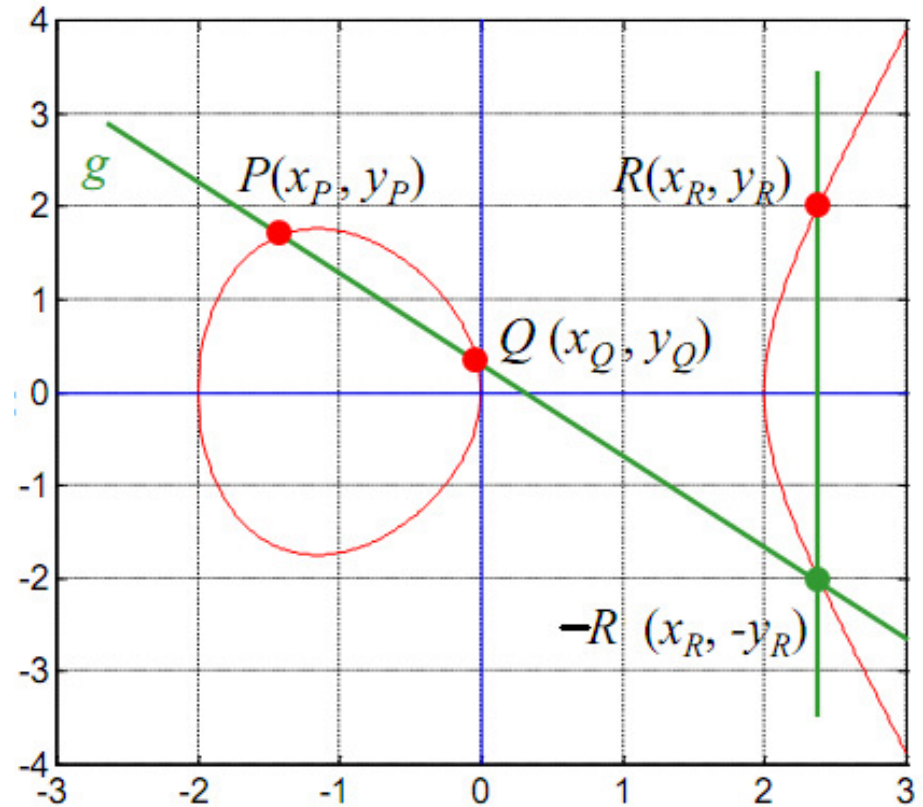
Perpotongan garis g dengan kurva:

$$(\lambda x + \beta)^2 = x^3 + ax + b$$

Koordinat Titik R:

$$x_r = \lambda^2 - x_p - x_q$$

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



Sumber gambar: Andreas Steffen, Elliptic Curve Cryptography

Contoh: Kurva eliptik $y^2 = x^3 + 2x + 4$

Misalkan $P(2, 4)$ dan $Q(0, 2)$ dua titik pada kurva

Penjumlahan titik: $P + Q = R$. Tentukan R !

Langkah-langkah menghitung koordinat R :

- Gradien garis g : $\lambda = (y_p - y_q)/(x_p - x_q) = (4 - 2)/(2 - 0) = 1$
- $x_r = \lambda^2 - x_p - x_q = 1^2 - 2 - 0 = -1$
- $y_r = \lambda(x_p - x_r) - y_p = 1(2 - (-1)) - 4 = -1$
- Jadi koordinat $R(-1, -1)$
- Periksa apakah $R(-1, -1)$ sebuah titik pada kurva eliptik:

$$y^2 = x^3 + 2x + 4 \iff (-1)^2 = (-1)^3 + 2(-1) + 4$$

$$\iff 1 = -1 - 2 + 4$$

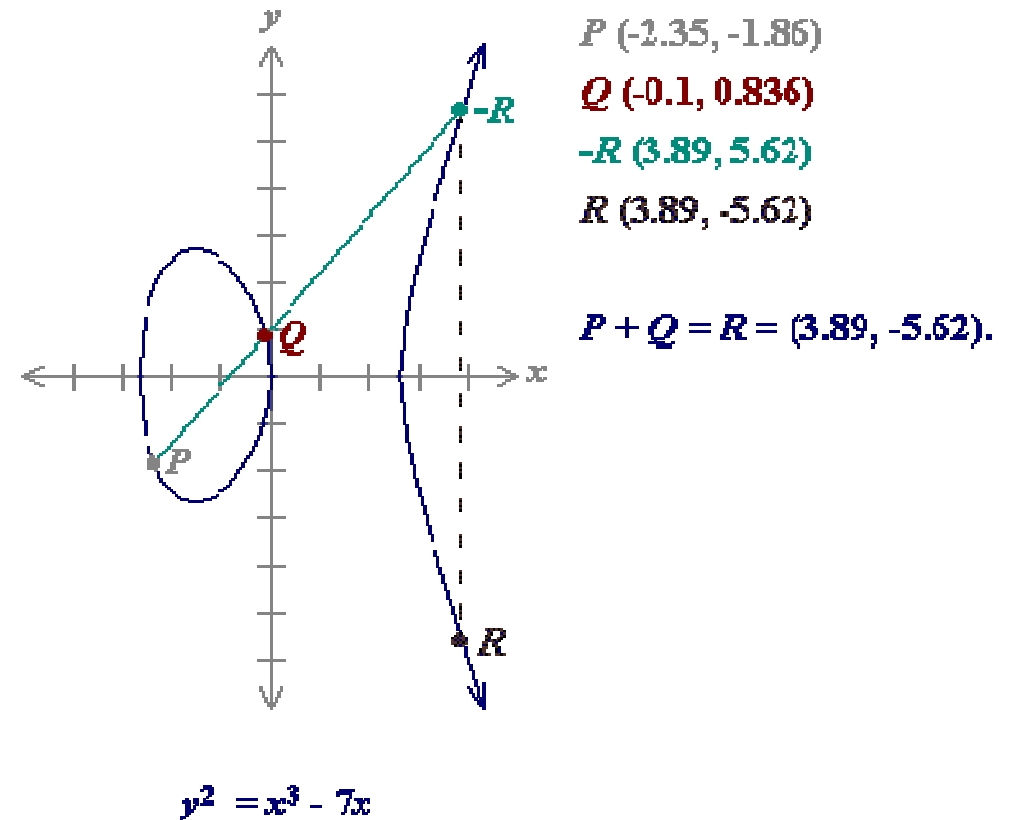
$$\iff 1 = 1 \quad (\text{terbukti } R(-1, -1) \text{ titik pada kurva } y^2 = x^3 + 2x + 4)$$

- Contoh lain:

$$\begin{aligned}\lambda &= (y_p - y_q)/(x_p - x_q) \\ &= (-1.86 - 0.836)/(-2.35 - (-0.1)) \\ &= -2.696 / -2.25 = 1.198\end{aligned}$$

$$\begin{aligned}x_r &= \lambda^2 - x_p - x_q \\ &= (1.198)^2 - (-2.35) - (-0.1) \\ &= 3.89\end{aligned}$$

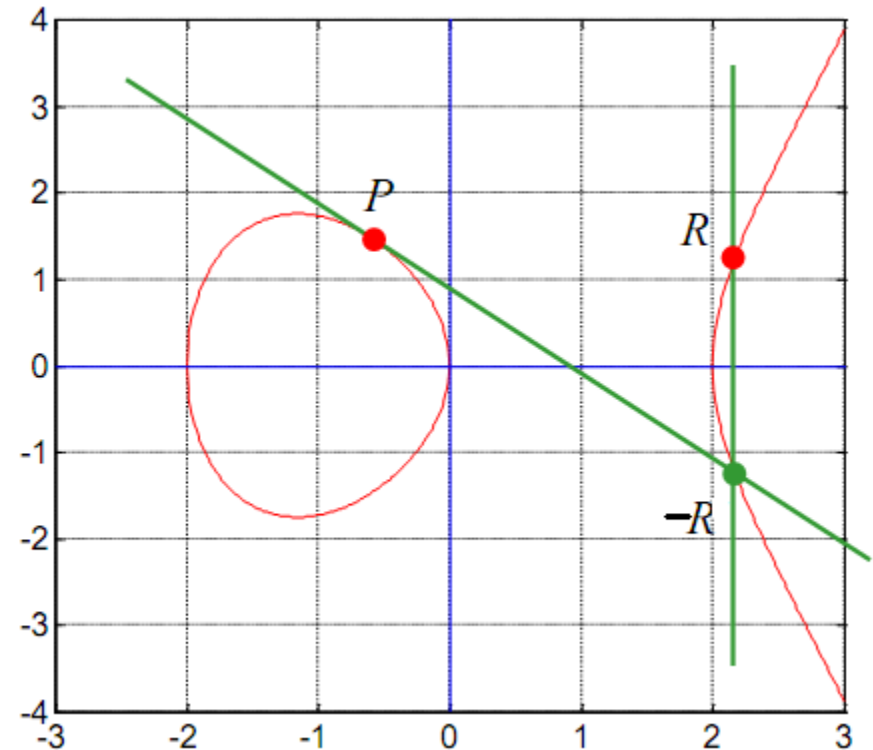
$$\begin{aligned}y_r &= \lambda(x_p - x_r) - y_p \\ &= 1.198(-2.35 - 3.89) - (-1.86) \\ &= -5.62\end{aligned}$$



Sumber gambar: **Debdeep Mukhopadhyay, Elliptic Curve Cryptography** ,
 Dept of Computer Sc and Engg IIT Madras

Penggandaan Titik

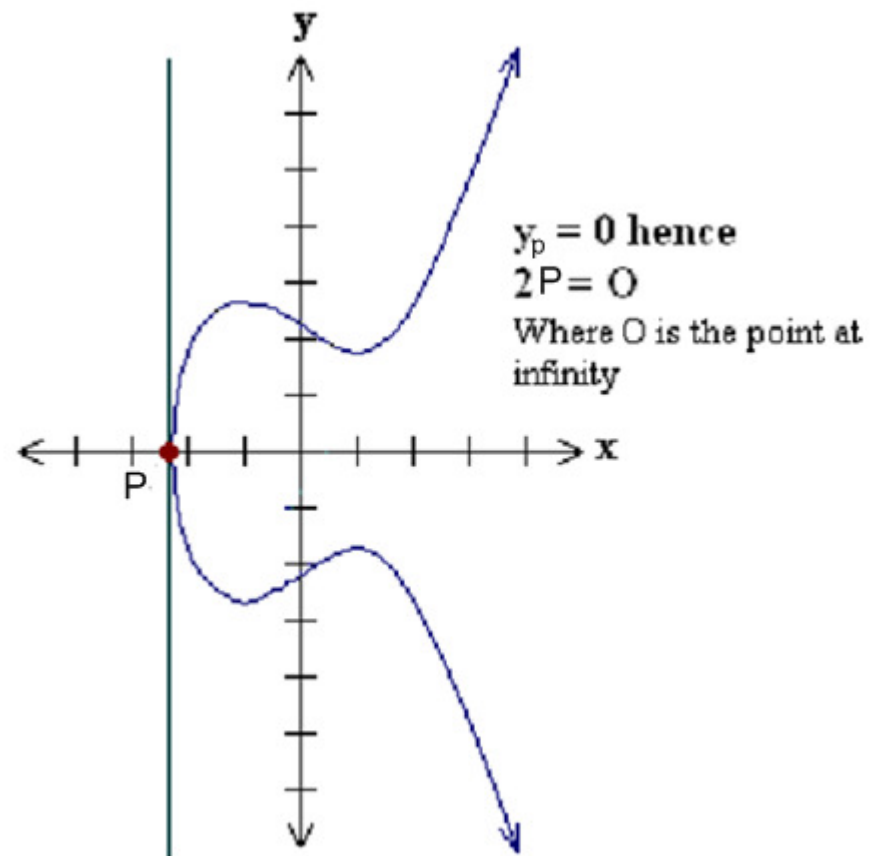
- Penggandaan titik (*point doubling*): menjumlahkan sebuah titik pada dirinya sendiri
- Penggandaan titik membentuk tangen pada titik $P(x, y)$
- $P + P = 2P = R$



Sumber gambar: Andreas Steffen, Elliptic Curve Cryptography

- Jika ordinat titik P nol, yaitu $y_p = 0$, maka tangen pada titik tersebut berpotongan pada sebuah titik di *infinity*.

- Di sini, $P + P = 2P = O$



Sumber gambar: Anoop MS ,
Elliptic Curve Cryptography,
an Implementation Guide

Penjelasan Analitik

Persamaan tangen g : $y = \lambda x + \beta$

$$\text{Gradien garis } g: \lambda = \frac{dy}{dx} = \frac{3x_p^2 + a}{2y_p}$$

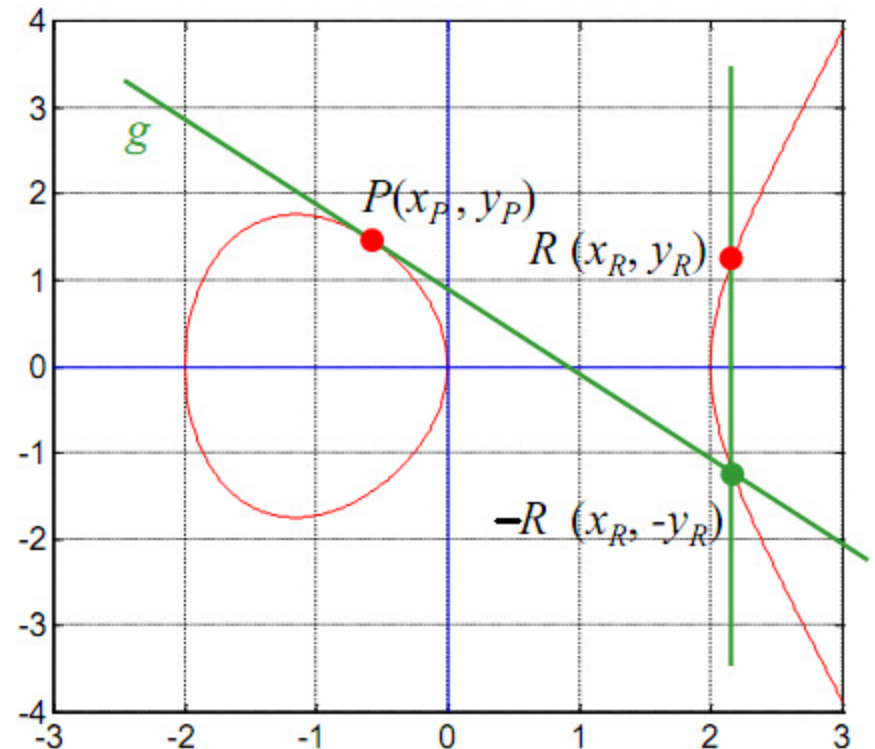
Perpotongan garis g dengan kurva: $(\lambda x + \beta)^2 = x^3 + ax + b$

Koordinat Titik R:

$$x_r = \lambda^2 - 2x_p$$

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

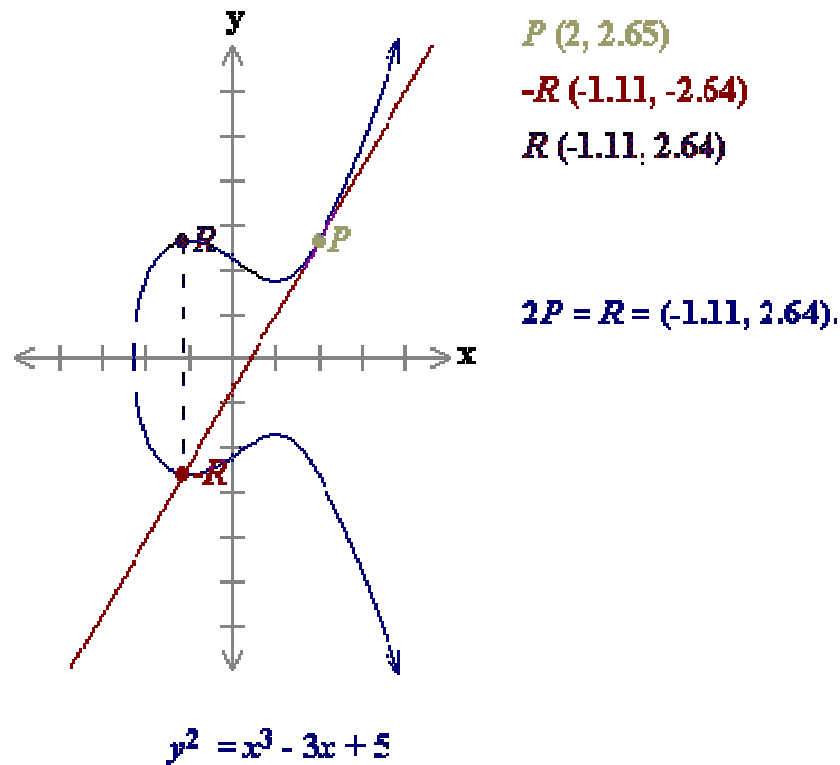
Jika $y_p = 0$ maka λ tidak terdefinisi sehingga $2P = O$



Sumber gambar: Andreas Steffen,
Elliptic Curve Cryptography

- Contoh:

$$P+P = 2P$$



Sumber gambar: **Debdeep Mukhopadhyay, Elliptic Curve Cryptography**,
 Dept of Computer Sc and Engg IIT Madras

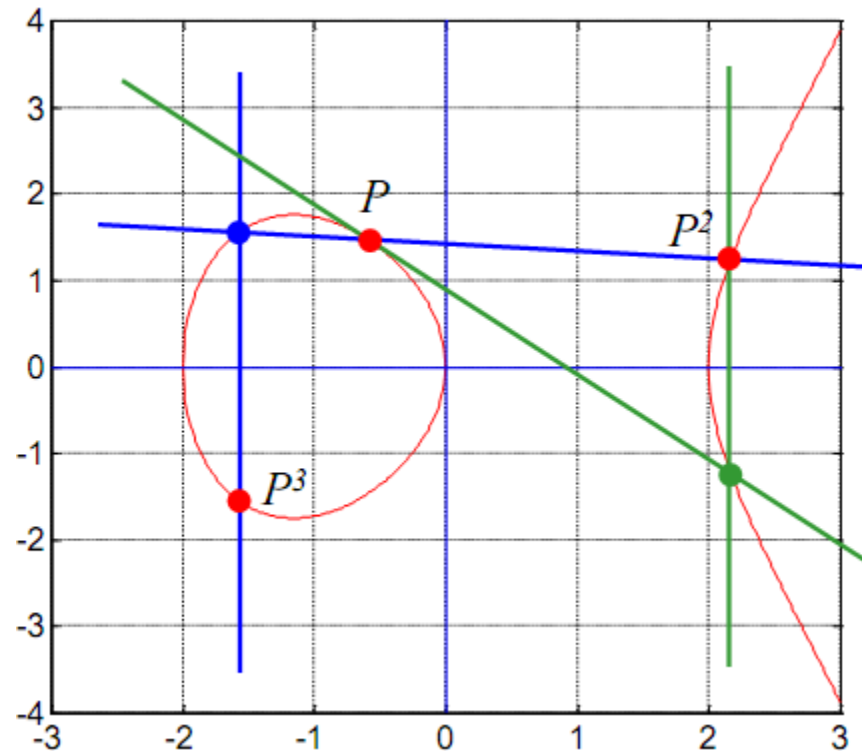
Pelelaran Titik

- Pelelaran titik (*point iteration*): menjumlahkan sebuah titik sebanyak $k - 1$ kali terhadap dirinya sendiri.

- $P^k = kP = P + P + \dots + P$

- Jika $k = 2 \rightarrow P^2 = 2P = P + P$

Sumber gambar: Andreas Steffen,
Elliptic Curve Cryptography



Jelaslah Kurva Eliptik membentuk Grup

$$\langle G, + \rangle$$

- Himpunan G : semua titik $P(x,y)$ pada kurva eliptik
- Operasi biner: $+$
- Semua aksioma terpenuhi sbb:
 1. Closure: semua operasi $P + Q$ berada di dalam G
 2. Asosiatif: $P + (Q + R) = (P + Q) + R$
 3. Elemen netral adalah O : $P + O = O + P = P$
 4. Elemen invers adalah $-P$: $P + (-P) = O$
 5. Komutatif: $P + Q = Q + P$ (abelian)

Perkalian Titik

- Perkalian titik: $kP = Q$

Ket: k adalah skalar, P dan Q adalah titik pada kurva eliptik

- Perkalian titik diperoleh dengan perulangan dua operasi dasar kurva eliptik yang sudah dijelaskan:
 1. Penjumlahan titik ($P + Q = R$)
 2. Penggandaan titik ($2P = R$)
- Contoh: $k = 3 \rightarrow 3P = P + P + P$ atau $3P = 2P + P$
 $k = 23 \rightarrow kP = 23P = 2(2(2(2P) + P) + P) + P$

Elliptic Curve Discrete Logarithm Problem (ECDLP)

- Menghitung $kP = Q$ mudah, tetapi menghitung k dari P dan Q sulit. Inilah ECDLP yang menjadi dasar ECC.
- ECDLP dirumuskan sebagai berikut:
Diberikan P dan Q adalah dua buah titik di kurva eliptik, carilah integer k sedemikian sehingga $Q = kP$
- Secara komputasi sulit menemukan k , jika k adalah bilangan yang besar. k adalah logaritma diskrit dari Q dengan basis P . *)
- Pada algoritma ECC, Q adalah kunci publik, k adalah kunci privat, dan P sembarang titik pada kurva eliptik.

Catatan: ingatlah $kP = P^k$, sehingga $Q = kP = P^k$, k adalah logaritma diskrit dari Q

Kurva Eliptik pada Galois Field

- Operasi kurva eliptik yang dibahas sebelum ini didefinisikan pada bilangan riil.
- Operasi pada bilangan riil tidak akurat karena mengandung pembulatan
- Pada sisi lain, kriptografi dioperasikan pada ranah bilangan integer.
- Agar kurva eliptik dapat dipakai di dalam kriptografi, maka kurva eliptik didefinisikan pada medan berhingga atau Galois Field, yaitu $GF(p)$ dan $GF(2^m)$.
- Yang dibahas dalam kuliah ini hanya kurva eliptik pada $GF(p)$

Kurva Eliptik pada GF(p)

- Bentuk umum kurva eliptik pada GF(p) (atau F_p) :

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

yang dalam hal ini p adalah bilangan prima dan elemen-elemen medan galois adalah $\{0, 1, 2, \dots, p - 1\}$

- **Contoh:** Tentukan semua titik $P(x,y)$ pada kurva eliptik $y^2 = x^3 + x + 6 \pmod{11}$ dengan x dan y didefinisikan di dalam $GF(11)$

Jawab:

$x = 0 \rightarrow y^2 = 6 \pmod{11} \rightarrow$ tidak ada nilai y yang memenuhi

$x = 1 \rightarrow y^2 = 8 \pmod{11} \rightarrow$ tidak ada nilai y yang memenuhi

$x = 2 \rightarrow y^2 = 16 \pmod{11} \equiv 5 \pmod{11} \rightarrow y_1 = 4$ dan $y_2 = 7$

$\rightarrow P(2,4)$ dan $P'(2, 7)$

$x = 3 \rightarrow y^2 = 36 \pmod{11} \equiv 3 \pmod{11} \rightarrow y_1 = 5$ dan $y_2 = 6$

$\rightarrow P(3,5)$ dan $P'(3, 6)$

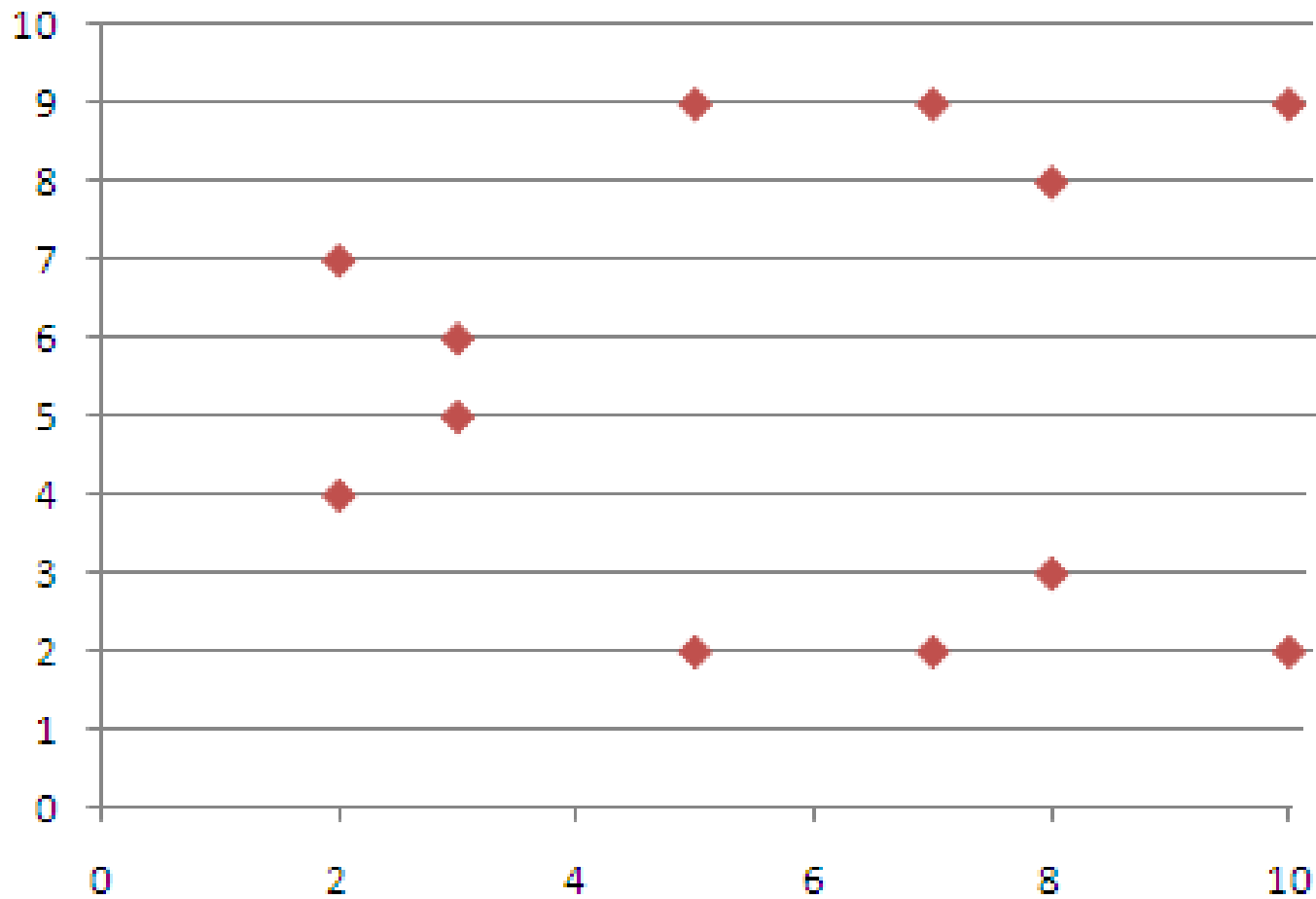
Jika diteruskan untuk $x = 4, 5, \dots, 10$, diperoleh tabel sebagai berikut :

x	y^2	$y_{1,2}$	$P(x, y)$	$P'(x, y)$
0	6	-		
1	8	-		
2	5	4, 7	(2, 4)	(2, 7)
3	3	5, 6	(3, 5)	(3, 6)
4	8	-		
5	4	2, 9	(5, 2)	(5, 9)
6	8	-		
7	4	2, 9	(7, 2)	(7, 9)
8	9	3, 8	(8, 3)	(8, 8)
9	7	-		
10	4	2, 9	(10, 2)	(10, 9)

Jadi, titik-titik yang terdapat pada kurva eliptik adalah 12, yaitu:
 $(2, 4), (2, 7), (3, 5), (3, 6), (5, 2), (5, 9), (7, 2), (7, 9), (8, 3), (8, 8), (10, 2), (10, 9)$

Jika ditambah dengan titik O di infinity, maka titik-titik pada kurva eliptik membentuk grup dengan $n = 13$ elemen.

Sumber: Andreas Steffen,
 Elliptic Curve Cryptography



Sebaran titik di dalam kurva eliptik $y^2 = x^3 + x + 6 \pmod{11}$ pada $GF(11)$

Penjumlahan Dua Titik di dalam EC pada GF(p)

Misalkan $P(x_p, y_p)$ dan $Q(x_q, y_q)$.

Penjumlahan: $P + Q = R$

Koordinat Titik R:

$$x_r = \lambda^2 - x_p - x_q \pmod p$$

$$y_r = \lambda(x_p - x_r) - y_p \pmod p$$

λ adalah gradien:

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

Pengurangan Dua Titik di dalam EC pada GF(p)

Misalkan $P(x_p, y_p)$ dan $Q(x_q, y_q)$.

Pengurangan: $P - Q = P + (-Q)$, yang dalam hal ini
 $-Q(x_q, -y_q \pmod{p})$.

Penggandaan Titik di dalam EC pada GF(p)

Misalkan $P(x_p, y_p)$ yang dalam hal ini $y_p \neq 0$.

Penggandaan titik: $2P = R$

Koordinat Titik R:

$$x_r = \lambda^2 - 2x_p \pmod p$$

$$y_r = \lambda(x_p - x_r) - y_p \pmod p$$

Yang dalam hal ini,

$$\lambda = \frac{3x_p + a}{2y_p} \pmod p$$

Jika $y_p = 0$ maka λ tidak terdefinisi sehingga $2P = O$

- **Contoh:** Misalkan $P(2, 4)$ dan $Q(5, 9)$ adalah dua buah titik pada kurva eliptik $y^2 = x^3 + x + 6 \pmod{11}$. Tentukan $P + Q$ dan $2P$.

Jawab:

$$\begin{aligned}\lambda &= (9 - 4)/(5 - 2) \pmod{11} = 5/3 \pmod{11} = 5 \cdot 3^{-1} \pmod{11} \\ &= 5 \cdot 4 \pmod{11} \equiv 9 \pmod{11}\end{aligned}$$

$P + Q = R$, koordinat Titik R:

$$x_r = \lambda^2 - x_p - x_q \pmod{11} = 81 - 2 - 5 \pmod{11} \equiv 8 \pmod{11}$$

$$\begin{aligned}y_r &= \lambda(x_p - x_r) - y_p \pmod{11} = 9(2 - 8) - 4 \pmod{11} = -58 \pmod{11} \\ &\equiv 8 \pmod{11}\end{aligned}$$

Jadi, $R(8, 8)$

Menghitung $2P = R$:

$$\begin{aligned}\lambda &= (3(2)^2 + 1)/8 \pmod{11} = 13/8 \pmod{11} \\ &= 13 \cdot 8^{-1} \pmod{11} \\ &= 13 \cdot 7 \pmod{11} \\ &= 78 \pmod{11} \equiv 3 \pmod{11}\end{aligned}$$

Koordinat R:

$$\begin{aligned}x_r &= 3^2 - 2 \cdot 2 \pmod{11} \equiv 5 \pmod{11} \\ y_r &= \lambda(x_p - x_r) - y_p \pmod{11} = 3(2 - 5) - 4 \pmod{11} \\ &= -13 \pmod{11} \equiv 9 \pmod{11}\end{aligned}$$

Jadi, $R(5, 9)$

- Nilai kP untuk $k = 2, 3, \dots$ diperlihatkan pada tabel:

k	kP
1	(2, 4)
2	(5, 9)
3	(8, 8)
4	(10, 9)
5	(3, 5)
6	(7, 2)
7	(7, 9)
8	(3, 6)
9	(10, 2)
10	(8, 3)
11	(5, 2)
12	(2, 7)
13	0

Jika diketahui P , maka kita bisa menghitung
 $Q = kP$

Jika persoalannya dibalik sbb:
 Diberikan P , maka tidak mungkin
 menghitung k bila Q diketahui



ECDLP

Elliptic Curve Cryptography (ECC) *)

- ECC adalah sistem kriptografi kunci-publik, sejenis dengan RSA, Rabin, ElGamal, D-H, dll.
- Setiap pengguna memiliki **kunci publik dan kunci privat**
 - Kunci publik untuk enkripsi atau untuk verifikasi tanda tangan digital
 - Kunci privat untuk dekripsi atau untuk menghasilkan tanda tangan digital
- Kurva eliptik digunakan sebagai perluasan sistem kriptografi kunci-publik yang lain:
 1. Elliptic Curve ElGamal (ECEG)
 2. Elliptic Curve Digital Signature (ECDSA)
 3. Eliiptic Curve Diffie-Hellman (ECDH)

*) Sumber bahan: **Debdeep Mukhopadhyay, Elliptic Curve Cryptography**,
Dept of Computer Sc and Engg IIT Madras

Penggunaan Kurva Eliptik di dalam Kriptografi

- Bagian inti dari sistem kriptografi kunci-publik yang melibatkan kurva eliptik adalah **grup eliptik** (himpunan titik-titik pada kurva eliptik dan sebuah operasi biner +).
- Operasi matematika yang mendasari:
 - Jika RSA mempunyai operasi perpangkatan sebagai operasi matematika yang mendasainya, maka
 - ECC memiliki operasi perkalian titik (penjumlahan berulang dua buah titik)

*) Sumber bahan: **Debdeep Mukhopadhyay, Elliptic Curve Cryptography**,
Dept of Computer Sc and Engg IIT Madras

- Dua pihak yang berkomunikasi menyepakati parameter data sebagai berikut:

1. Persamaan kurva eliptik $y^2 = x^3 + ax + b \pmod p$

- Nilai a dan b
- Bilangan prima p

2. Grup eliptik yang dihitung dari persamaan kurva eliptik

3. Titik basis (*base point*) $B (x_B, y_B)$, dipilih dari grup eliptik untuk operasi kriptografi.

- Setiap pengguna membangkitkan pasangan kunci publik dan kunci privat

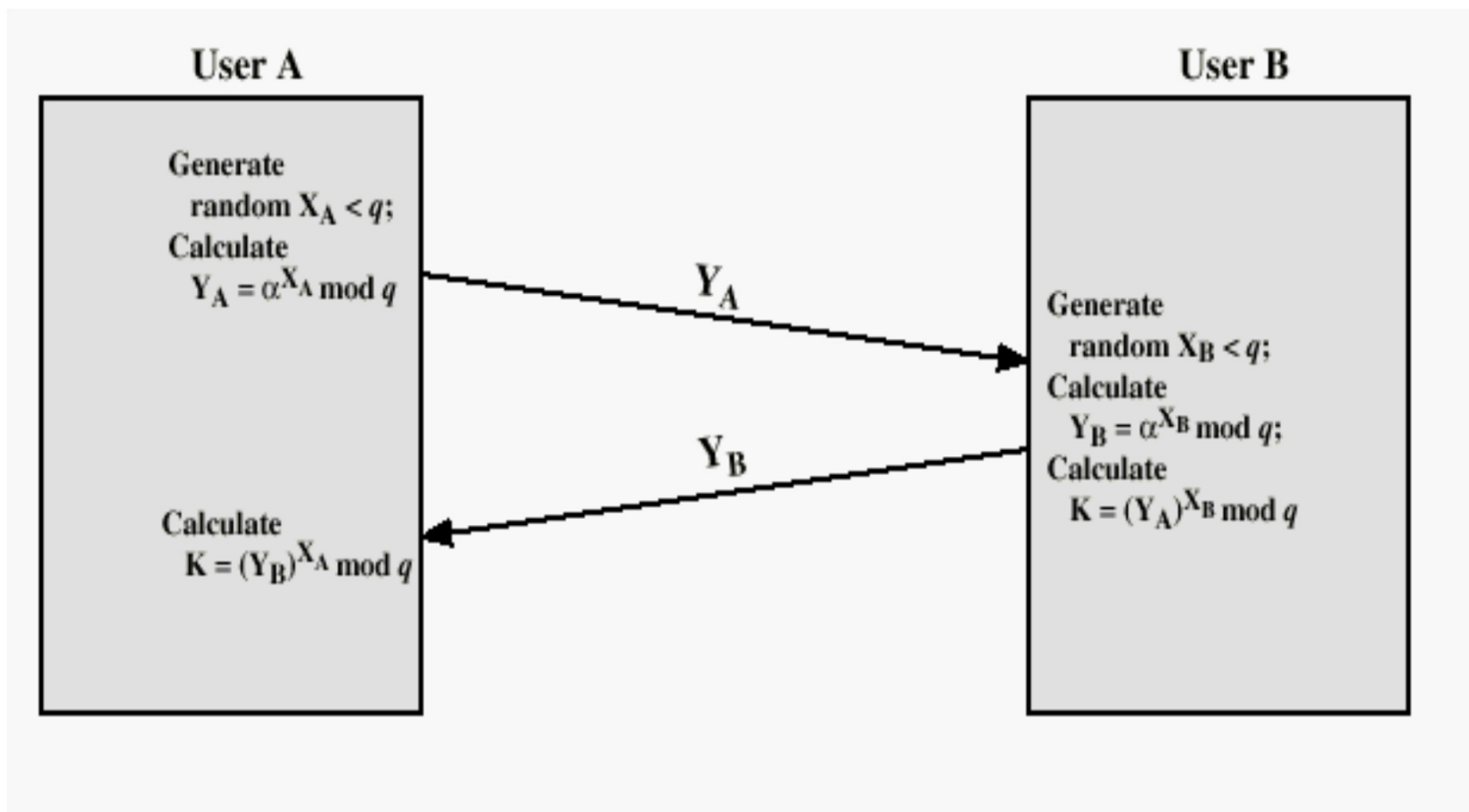
- Kunci privat = integer x , dipilih dari selang $[1, p - 1]$
- Kunci publik = titik Q , adalah hasil kali antara x dan titik basis B :

$$Q = x \cdot B$$

***) Sumber bahan: Debdeep Mukhopadhyay, Elliptic Curve Cryptography ,
Dept of Computer Sc and Engg IIT Madras**

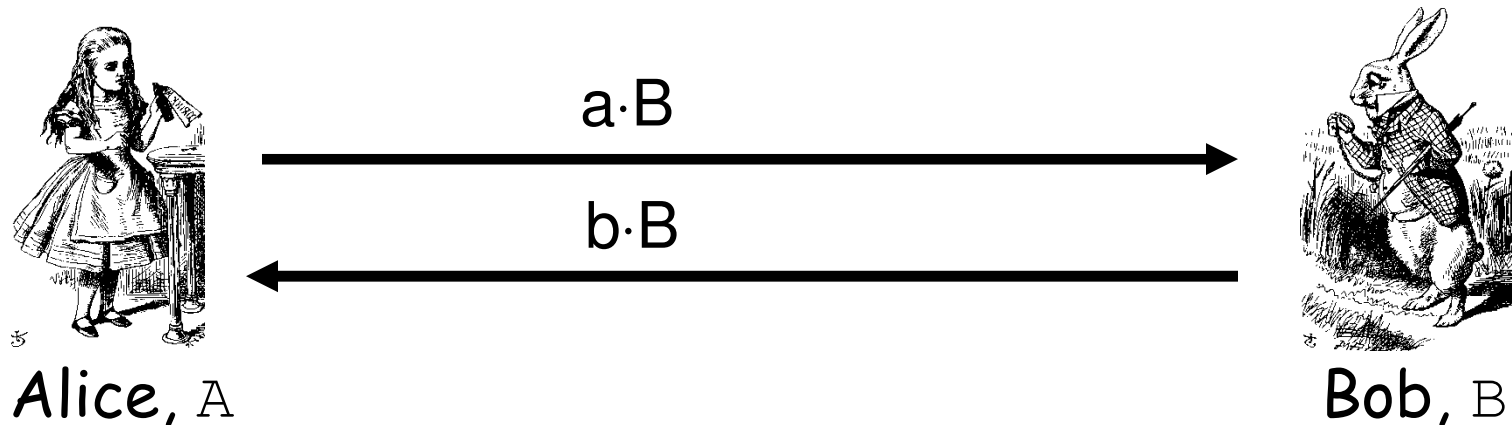
Review: Algoritma Diffie-Hellman

Ingatlah kembali diagram pertukaran kunci Diffie-Hellman:



Elliptic Curve Diffie-Hellman (ECDH)

- **Public:** Kurva eliptik dan titik $B(x,y)$ pada kurva
- **Secret:** Integer milik Alice, a , dan integer milik Bob, b



- Alice menghitung $a \cdot (b \cdot B)$
- Bob menghitung $b \cdot (a \cdot B)$
- Hasil perhitungan akan sama karena $ab = ba$

*) Sumber bahan: **Debdeep Mukhopadhyay, Elliptic Curve Cryptography**,
Dept of Computer Sc and Engg IIT Madras

Algoritma Elliptic Curve Diffie-Hellman

- Alice dan Bob ingin berbagi sebuah kunci rahasia.
 - Alice dan Bob menghitung kunci publik dan kunci privat masing-masing.
 - Alice
 - » Kunci privat = a
 - » Kunci publik = $P_A = a \cdot B$
 - Bob
 - » Kunci privat = b
 - » Kunci publik = $P_B = b \cdot B$
 - Alice dan Bob saling mengirim kunci publik masing-masing.
 - Keduanya melakukan perkalian kunci privatnya dengan kunci publik mitranya untuk mendapatkan kunci rahasia yang mereka bagi
 - Alice $\rightarrow K_{AB} = a(bB)$
 - Bob $\rightarrow K_{AB} = b(aB)$
 - **Kunci rahasia = $K_{AB} = abB$**

*) Sumber bahan: **Debdeep Mukhopadhyay, Elliptic Curve Cryptography**,
Dept of Computer Sc and Engg IIT Madras

Contoh *): Misalkan kurva eliptik yang dipilih adalah $y^2 = x^3 + 2x + 1$ dan $p = 5$. Himpunan titik-titik pada kurva eliptik adalah $\{(0, 1), (1, 3), (3, 3), (3, 2), (1, 2), (0, 4)\}$. Alice dan Bob menyepakatai titik $B(0, 1)$ sebagai basis.

1. Alice memilih $a = 2$, lalu menghitung kunci publiknya:

$$P_A = a \cdot B = 2B = B + B = (1, 3) \rightarrow \text{misalkan titik } Q$$

2. Bob memilih $b = 3$, lalu menghitung kunci publiknya:

$$P_B = b \cdot B = 3B = B + B + B = 2B + B = (3, 3) \rightarrow \text{misalkan titik } R$$

3. Alice mengirimkan P_A kepada Bob, Bob mengirimkan P_B kepada Alice.

4. Alice menghitung kunci rahasia sbb:

$$K_A = a \cdot P_B = 2R = R + R = (0, 4)$$

5. Bob menghitung kunci rahasia sbb:

$$K_B = b \cdot P_A = 2Q = Q + Q = (0, 4)$$

Jadi, sekarang Alice dan Bob sudah berbagi kunci rahasia yang sama, yaitu $(0, 4)$

***) Sumber bahan: Nana Juhana, Implementasi Elliptic Curve Cryptography (ECC) pada proses Pertukaran Kunci Diffie-Hellman dan Skema Enkripsi El Gamal**

Elliptic Curve El Gamal

- *Elliptic Curve El Gamal*: sistem kriptografi kurva eliptik yang analog dengan El Gamal.
- Misalkan **Alice** ingin mengirim **Bob** pesan yang dienkripsi.
 - Baik Alice dan Bob menyepakati titik basis B .
 - Alice dan Bob membuat kunci privat/kunci publik.
 - Alice
 - Kunci privat = a
 - Kunci publik = $P_A = a * B$
 - Bob
 - Kunci privat = b
 - Kunci publik = $P_B = b * B$
 - Alice mengambil plaintext, M , lalu mengkodekannya menjadi sebuah titik, P_M , dari kurva eliptik

*) Sumber bahan: **Debdeep Mukhopadhyay, Elliptic Curve Cryptography**,
Dept of Computer Sc and Engg IIT Madras

- Alice memilih bilangan acak lain, k , dari selang $[1, p-1]$
 - Cipherteks adalah pasangan titik
 - $P_C = [(kB), (P_M + kP_B)]$
 - Untuk mendekripsi, Bob mula-mula menghitung hasil kali titik pertama P_C dengan kunci privatnya, b
 - $b \cdot (kB)$
-

- Bob kemudian mengurangkan titik kedua dari P_C dengan hasil kali di atas
 - $(P_M + kP_B) - [b \cdot (kB)] = P_M + k \cdot (bB) - b \cdot (kB) = P_M$
- Bob kemudian men-*decode* P_M untuk memperoleh pesan M

*) Sumber bahan: **Debdeep Mukhopadhyay, Elliptic Curve Cryptography**,
Dept of Computer Sc and Engg IIT Madras

Perbandingan El Gamal dengan Elliptic Curve El Gamal

- Cipherteks pada EC El Gamal adalah pasangan titik
 - $P_C = [(kB), (P_M + kP_B)]$

- Cipherteks pada El Gamal juga pasangan nilai:

- $C = (g^k \text{ mod } p, my_B^k \text{ mod } p)$ (ket: $y_b =$ kunci publik Bob)
-

- Bob kemudian mengurangkan titik kedua dari P_C dengan hasil kali **$b \cdot (kB)$**

- $(P_M + kP_B) - [b(kB)] = P_M + k(bB) - b(kB) = P_M$

- Di dalam El Gamal, Bob menghitung bagi dari nilai kedua dengan nilai pertama yang dipangkatkan dengan kunci privat Bob

- $m = my_B^k / (g^k)^b = mg^{k*b} / g^{k*b} = m$

*) Sumber bahan: **Debdeep Mukhopadhyay, Elliptic Curve Cryptography**,
Dept of Computer Sc and Engg IIT Madras

Keamanan ECC

- Untuk mengenkripsi kunci AES sepanjang 128-bit dengan algoritma kriptografi kunci publik:
 - Ukuran kunci RSA: 3072 bits
 - Ukuran kunci ECC: 256 bits
- Bagaimana cara meningkatkan keamanan RSA?
 - Tingkatkan ukuran kunci
- **Tidak Praktis?**

NIST guidelines for public key sizes for AES			
ECC KEY SIZE (Bits)	RSA KEY SIZE (Bits)	KEY SIZE RATIO	AES KEY SIZE (Bits)
163	1024	1 : 6	
256	3072	1 : 12	128
384	7680	1 : 20	192
512	15 360	1 : 30	256

Supplied by NIST to ANSI X9F1

*) Sumber bahan: **Debdeep Mukhopadhyay, Elliptic Curve Cryptography** ,
Dept of Computer Sc and Engg IIT Madras

Aplikasi ECC

- Banyak piranti yang berukuran kecil dan memiliki keterbatasan memori dan kemampuan pemrosesan.
- Di mana kita dapat menerapkan ECC?
 - Piranti komunikasi nirkabel
 - *Smart cards*
 - Web server yang membutuhkan penanganan banyak sesi enkripsi
 - **Sembarang aplikasi yang membutuhkan keamanan tetapi memiliki kekurangan dalam *power, storage and kemampuan komputasi* adalah potensial memerlukan ECC**

*) Sumber bahan: **Debdeep Mukhopadhyay, Elliptic Curve Cryptography** ,
Dept of Computer Sc and Engg IIT Madras

Keuntungan ECC

- Keuntungan yang sama dengan sistem kriptografi lain: *confidentiality, integrity, authentication and non-repudiation*, tetapi...
- Panjang kuncinya lebih pendek
 - Mempercepat proses *encryption, decryption*, dan *signature verification*
 - Penghematan *storage* dan *bandwidth*

*) Sumber bahan: **Debdeep Mukhopadhyay, Elliptic Curve Cryptography** ,
Dept of Computer Sc and Engg IIT Madras

Summary of ECC

- **“Hard problem”** analogous to discrete log
 - $Q=kP$, where Q, P belong to a prime curve
 - given $k, P \rightarrow$ “easy” to compute Q
 - given $Q, P \rightarrow$ “hard” to find k
 - known as the **elliptic curve logarithm problem**
 - k must be large enough
- ECC security relies on elliptic curve logarithm problem
 - compared to factoring, can use much smaller key sizes than with RSA etc
 - \rightarrow for similar security ECC offers significant computational advantages**