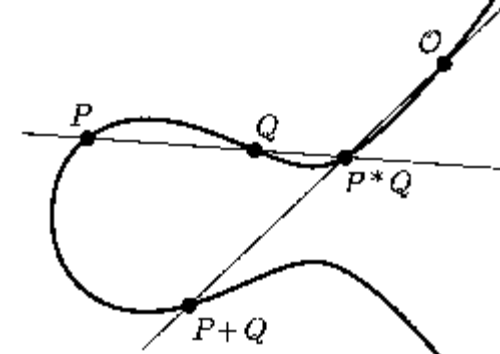


II4031 Kriptografi dan Koding



# Elliptic Curve Cryptography (ECC)

(Bagian 2)



Oleh: Rinaldi Munir

Program Studi Sistem dan Teknologi Informasi  
Sekolah Teknik Elektro dan Informatika

ITB

# Kurva Eliptik

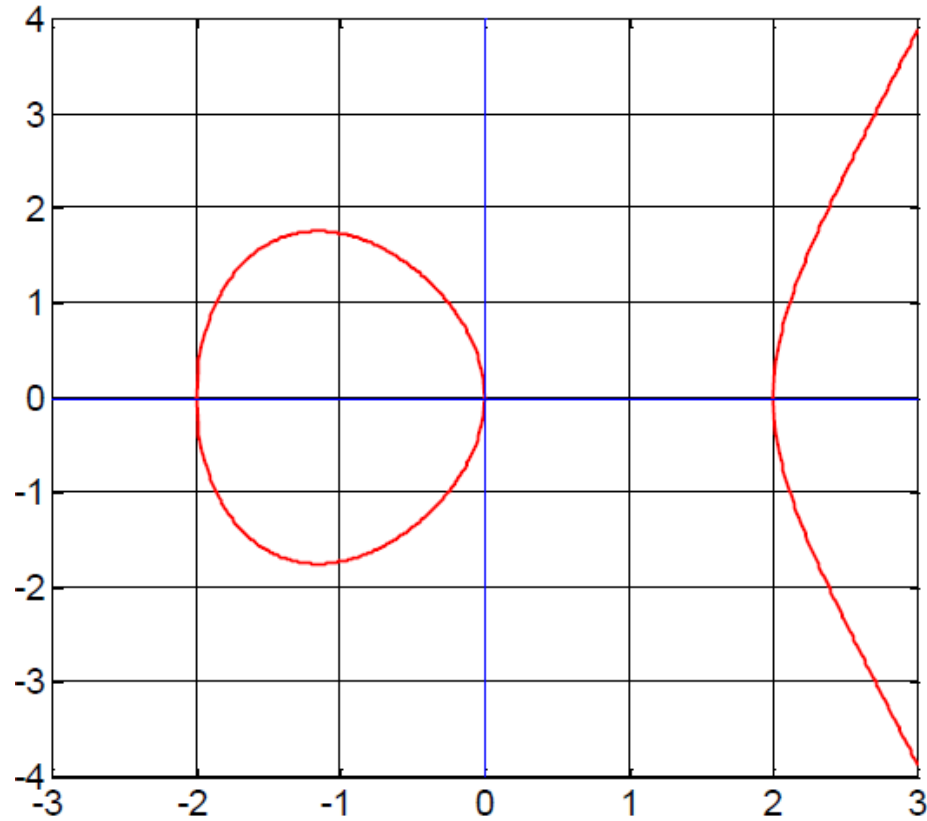
- Kurva eliptik adalah kurva dengan bentuk umum persamaan:

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

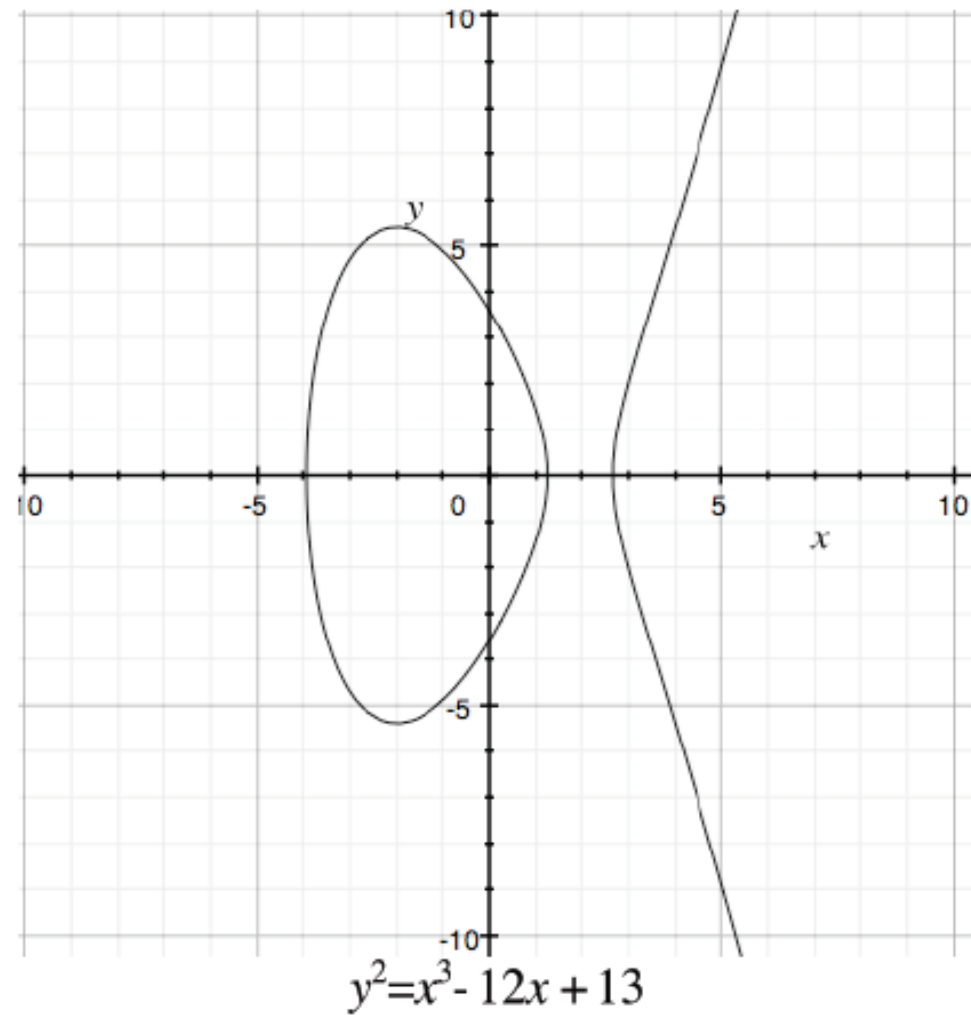
dengan syarat  $4a^3 + 27b^2 \neq 0$

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

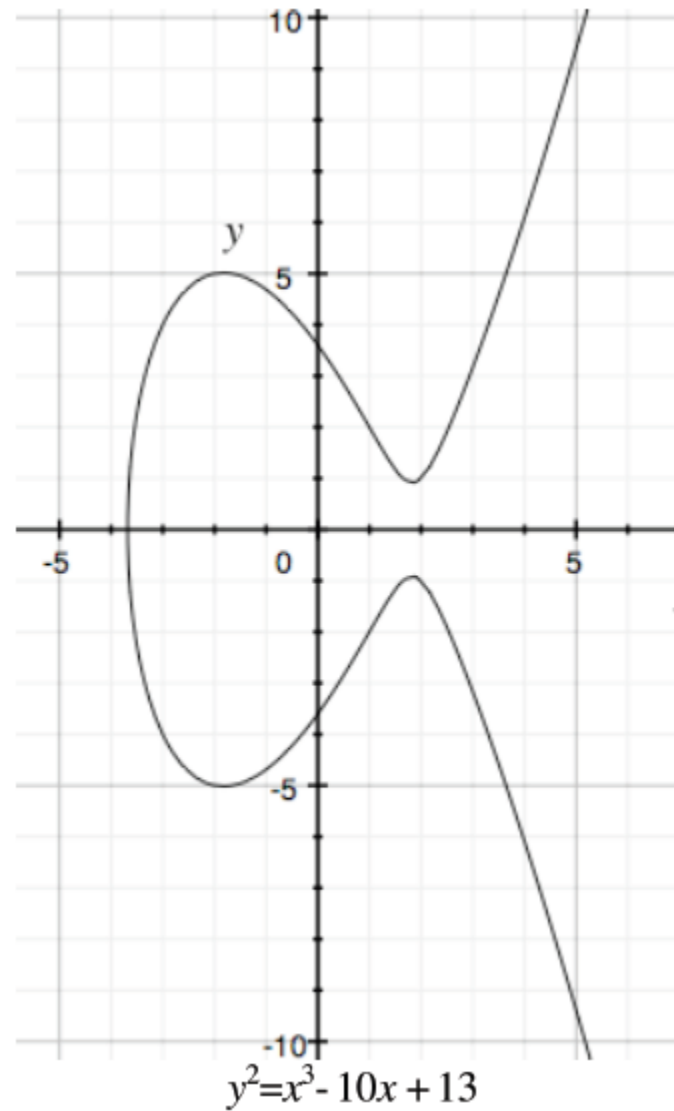
- Contoh:  $y^2 = x^3 - 4x$   
 $= x(x - 2)(x + 2)$



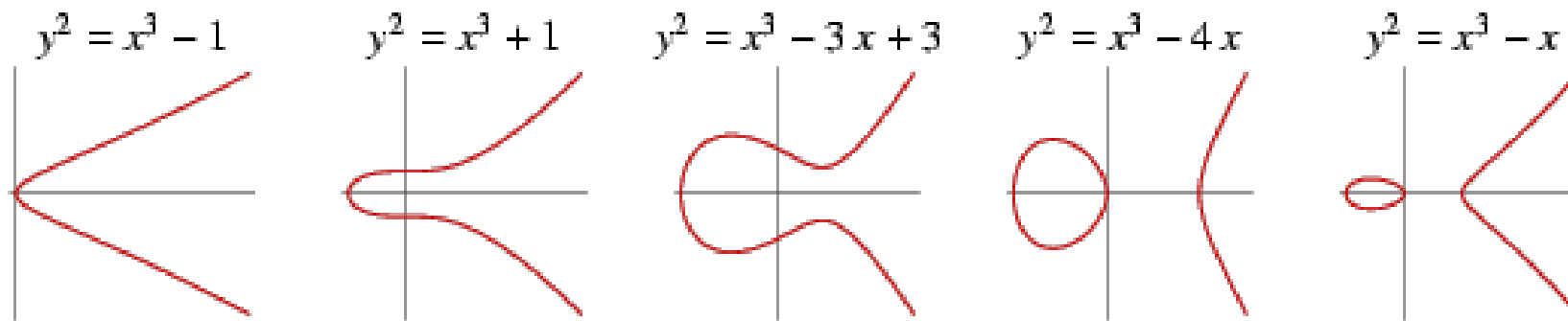
Sumber gambar: Andreas Steffen, Elliptic Curve Cryptography



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  $y^2 = x^3 + ax + b$  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  $G$  : semua titik  $P(x, y)$  pada kurva eliptik
  - Operasi biner :  $+$
- Penjelasan kenapa kurva eliptik membentuk sebuah grup dijelaskan pada *slide-slide* berikut ini.

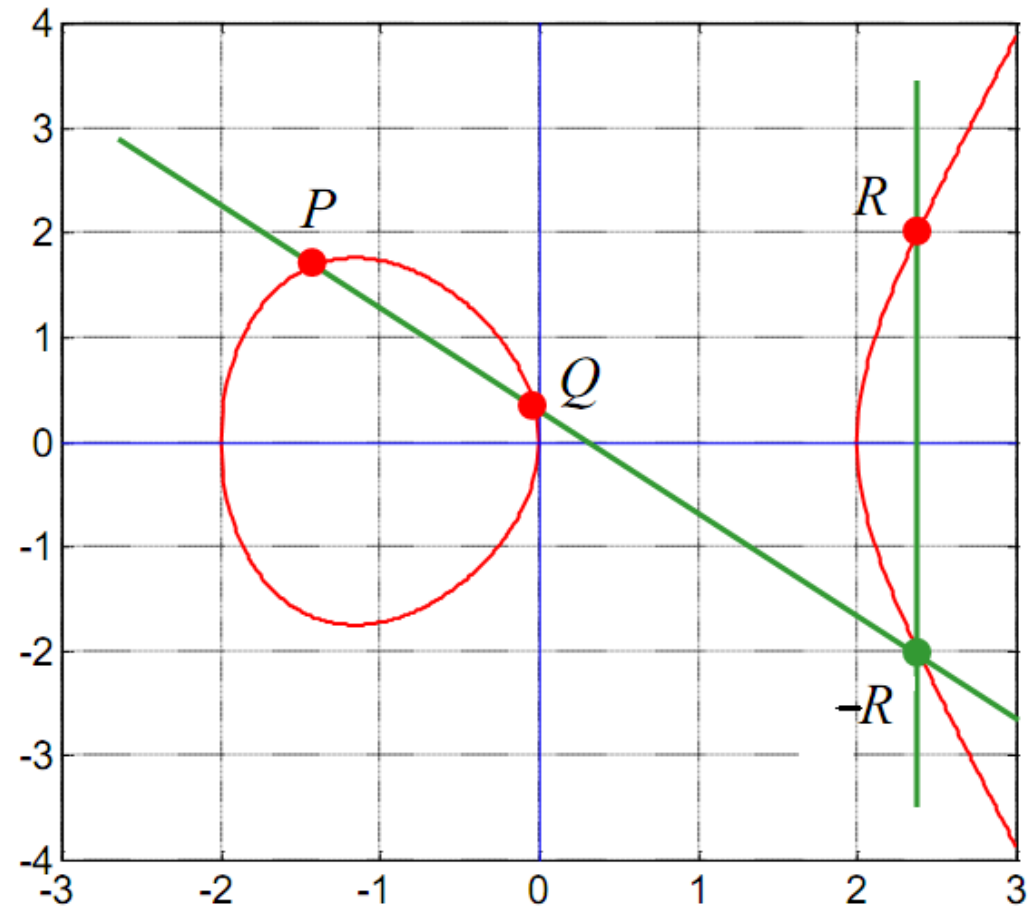
# Penjumlahan Titik pada Kurva Eliptik

## (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



# Penjelasan Analitik $P + Q = R$

Persamaan garis  $g$ :  $y = mx + c$

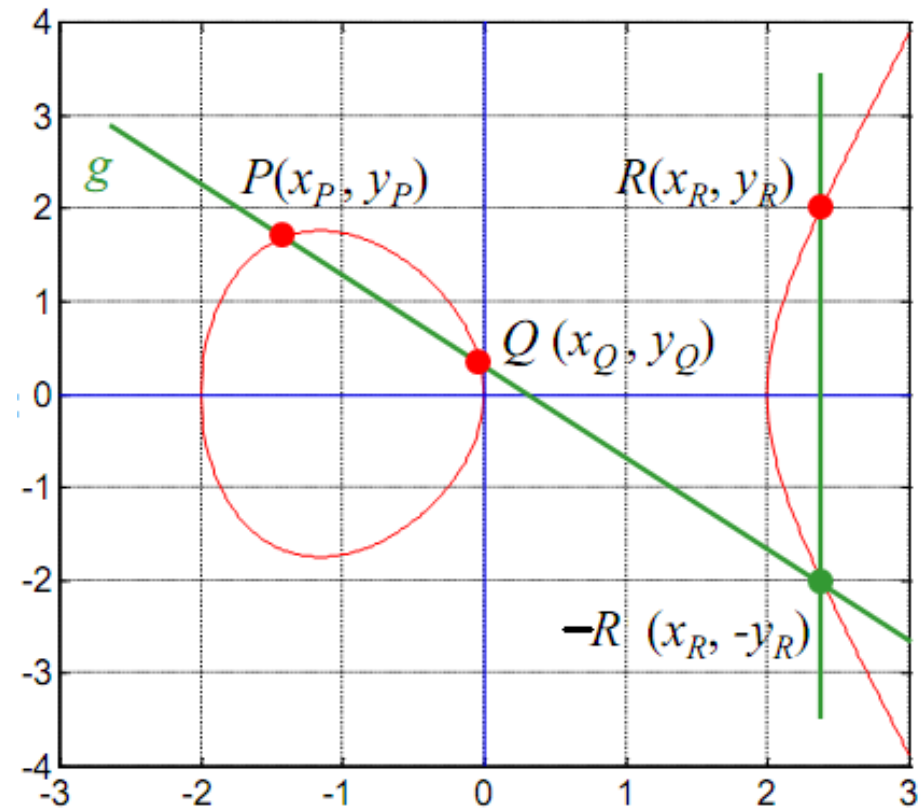
Gradien garis  $g$ :  $m = \frac{y_p - y_q}{x_p - x_q}$

Perpotongan garis  $g$  dengan  
kurva  $y^2 = x^3 + ax + b$ :  
 $(mx + c)^2 = x^3 + ax + b$

Koordinat Titik  $R$ :

$$x_r = m^2 - x_p - x_q$$

$$y_r = m(x_p - x_r) - y_p$$



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

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

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

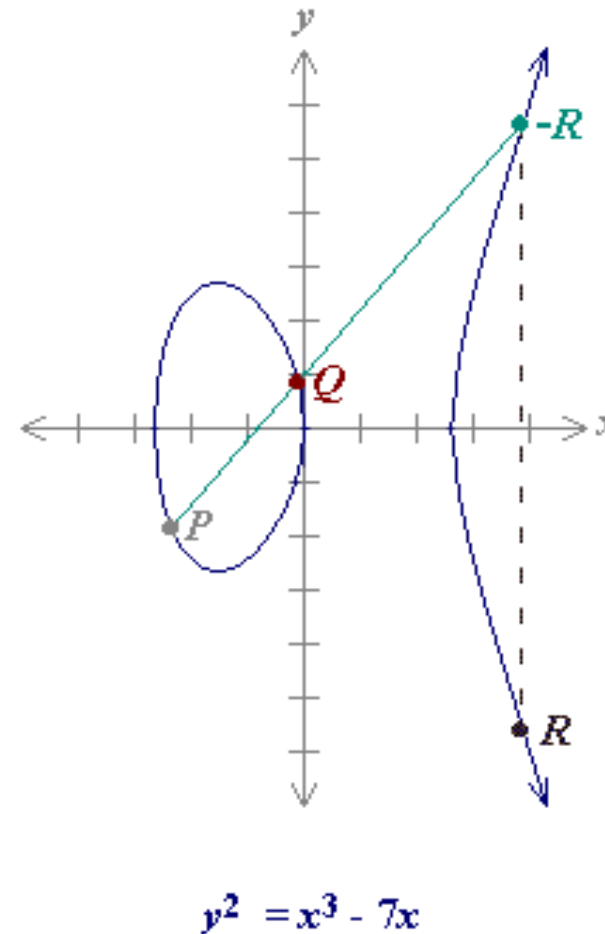
$$\Leftrightarrow 1 = 1 \quad (\text{terbukti } R(-1, -1) \text{ titik pada kurva } y^2 = x^3 + 2x + 4)$$

- Contoh lain:

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

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

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



$P (-2.35, -1.86)$

$Q (-0.1, 0.836)$

$-R (3.89, 5.62)$

$R (3.89, -5.62)$

$P + Q = R = (3.89, -5.62).$

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

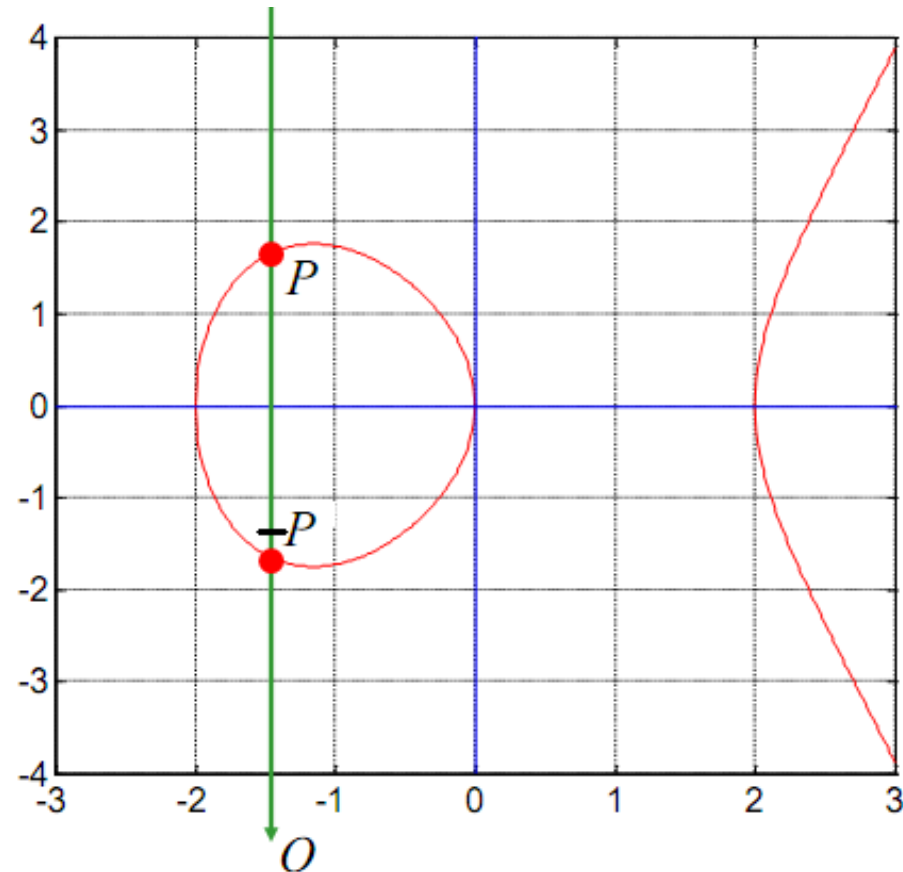
(b)  $P + (-P) = O$ , di sini  $O$  adalah titik di *infinity*

$P' = -P$  adalah elemen invers:

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

$O$  adalah elemen netral:

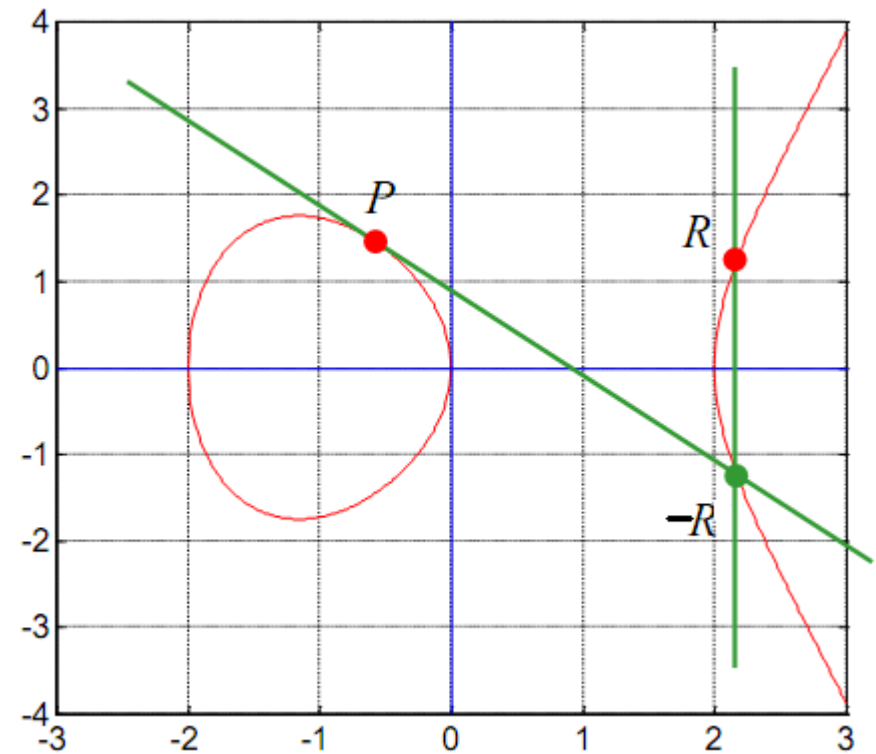
$$P + O = O + P = P$$



Sumber gambar: Andreas Steffen, Elliptic Curve Cryptography

# Penggandaan Titik

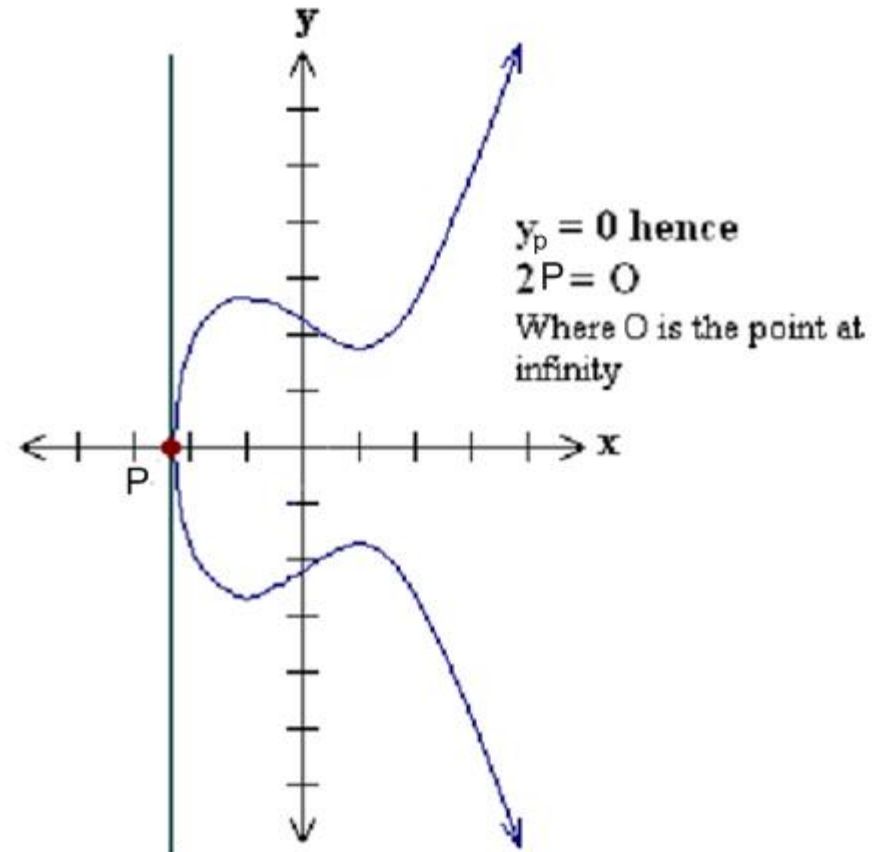
- Penggandaan titik (*point doubling*): menjumlahkan sebuah titik pada dirinya sendiri
- Penggandaan titik membentuk tangen pada titik  $P(x, y)$
- $P + P = 2P = R$



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 $P + P = 2P = R$

Persamaan tangen  $g$ :  $y = mx + c$

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

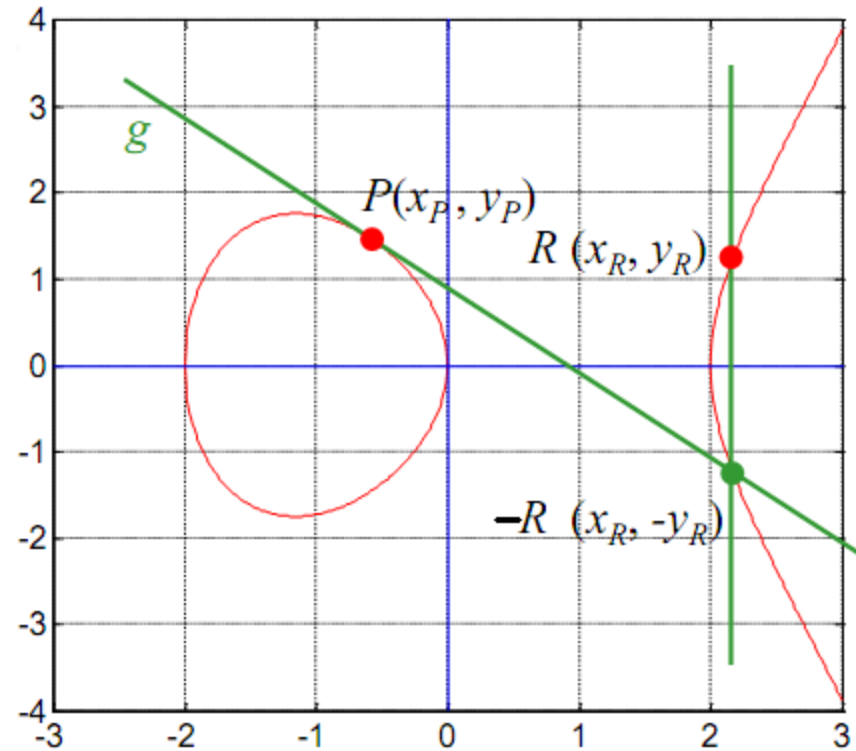
Perpotongan garis  $g$  dengan kurva:  $(mx + c)^2 = x^3 + ax + b$

Koordinat Titik  $R$ :

$$x_r = m^2 - 2x_p$$

$$y_r = m(x_p - x_r) - y_p$$

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



Sumber gambar: Andreas Steffen,  
Elliptic Curve Cryptography

- Contoh:

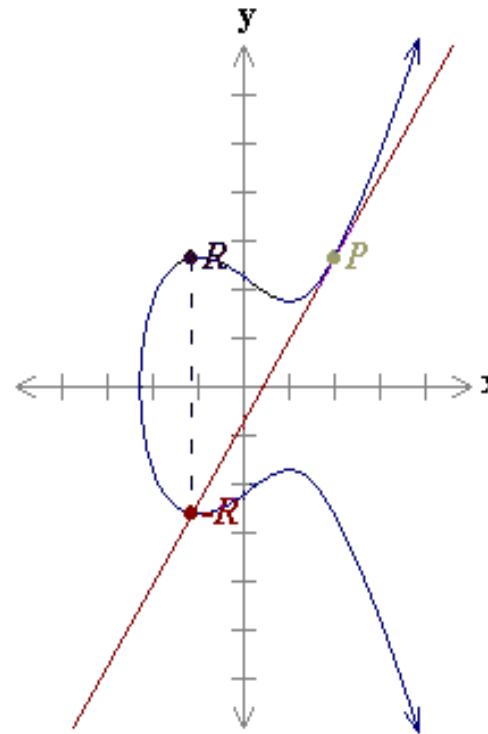
$$P+P = 2P$$

$$m = \frac{dy}{dx} = \frac{3x_p^2 + a}{2y_p}$$

Koordinat Titik R:

$$x_r = m^2 - 2x_p$$

$$y_r = m(x_p - x_r) - y_p$$



$P (2, 2.65)$

$-R (-1.11, -2.64)$

$R (-1.11, 2.64)$

$2P = R = (-1.11, 2.64).$

$$y^2 = x^3 - 3x + 5$$

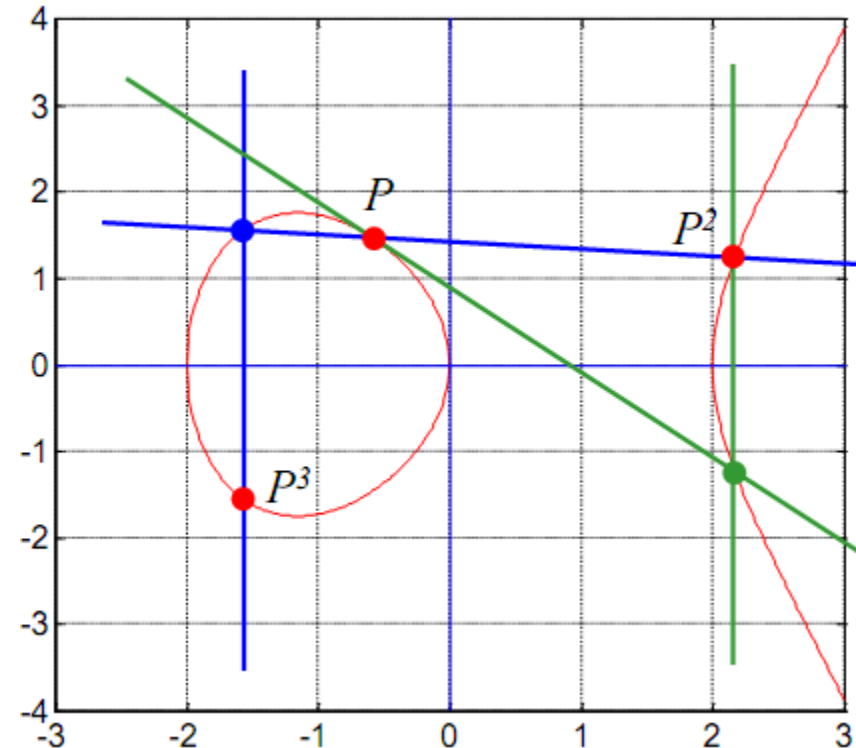
Sumber gambar: **Debdeep Mukhopadhyay, Elliptic Curve Cryptography**,  
Dept of Computer Sc and Engg IIT Madras



# 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 :

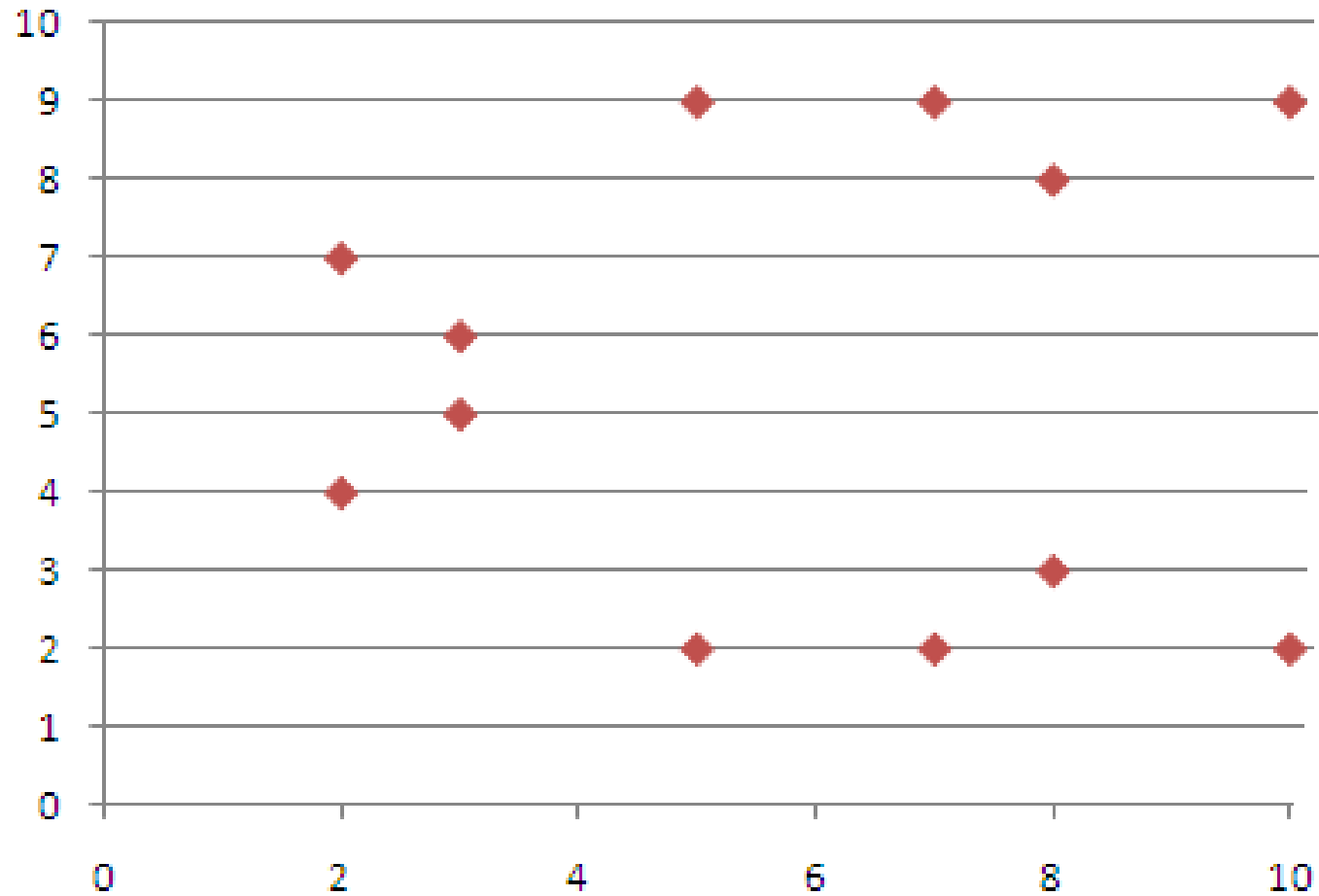
$x$	$y^2$	$y_{1,2}$	$P(x, y)$	$P'(x, y)$
0	6	-		
1	8	-		
2	5	4, 7	(2, 4)	(2, 7)
3	3	5, 6	(3, 5)	(3, 6)
4	8	-		
5	4	2, 9	(5, 2)	(5, 9)
6	8	-		
7	4	2, 9	(7, 2)	(7, 9)
8	9	3, 8	(8, 3)	(8, 8)
9	7	-		
10	4	2, 9	(10, 2)	(10, 9)

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.

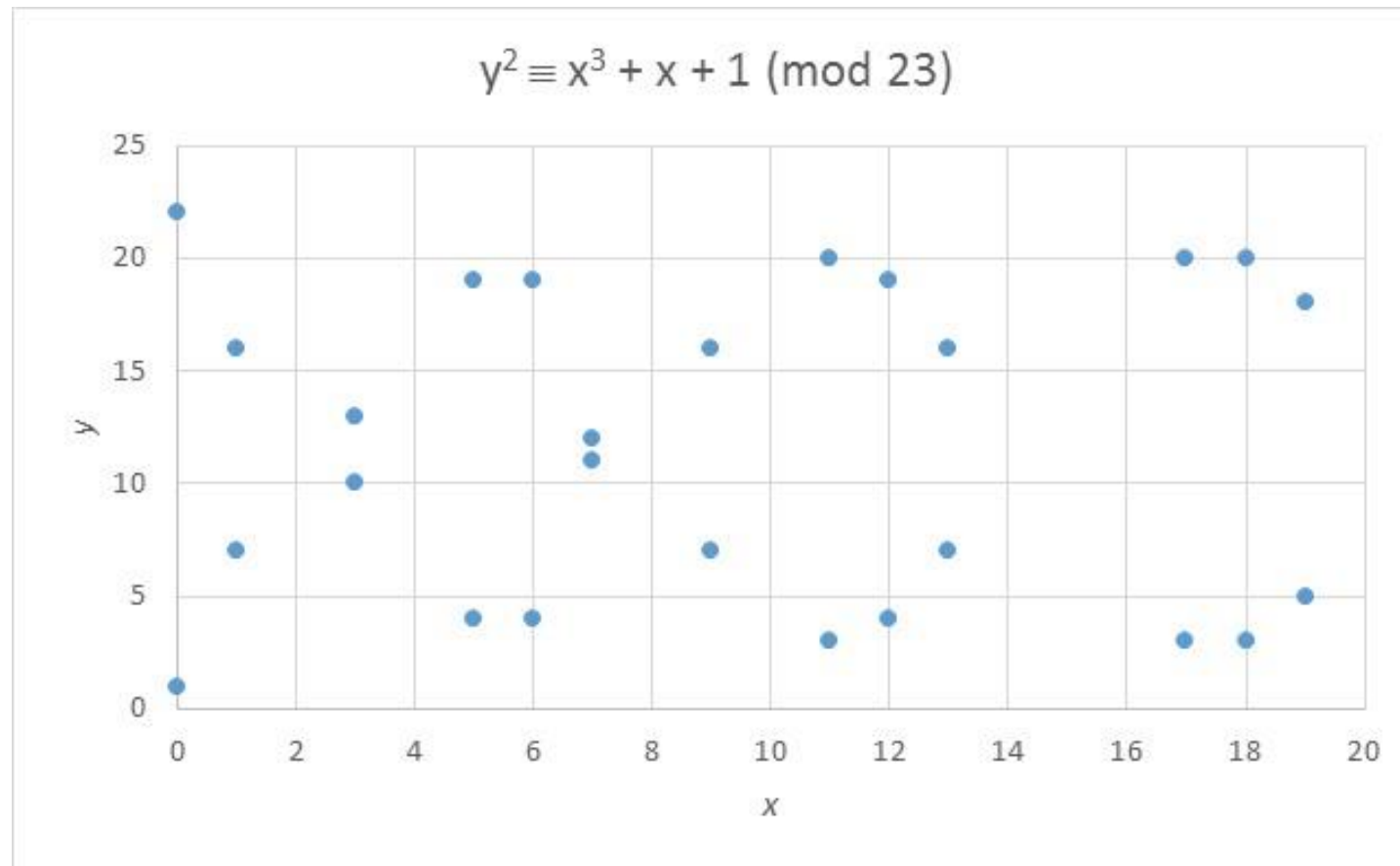
Sumber: Andreas Steffen,  
 Elliptic Curve Cryptography





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

- Contoh lain: Kurva eliptik  $y^2 \equiv x^3 + x + 1 \pmod{23}$  memiliki titik-titik di dalam himpunan  $\{(0, 1), (0, 22), (1, 7), (1, 16), (3, 10), (3, 13), (5, 4), (5, 19), (6, 4), (6, 19), (7, 11), (7, 12), (9, 7), (9, 16), (11, 3), (11, 20), (12, 4), (12, 19), (13, 7), (13, 16), (17, 3), (17, 20), (18, 3), (18, 20), (19, 5), (19, 18)\}$ .



## 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:

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

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

$m$  adalah gradien:

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

## 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:

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

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

Yang dalam hal ini,

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

Jika  $y_p = 0$  maka  $m$  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:

(a)  $P + Q = R$

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

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

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

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

Jadi,  $R(8, 8)$

(b)  $2P = R$

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

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

Koordinat R:

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

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  $P$  dan  $Q$ , maka sangat sukar  
menghitung  $k$  sedemikian sehingga  $Q = kP$



**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. Elliptic 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 (kP)

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

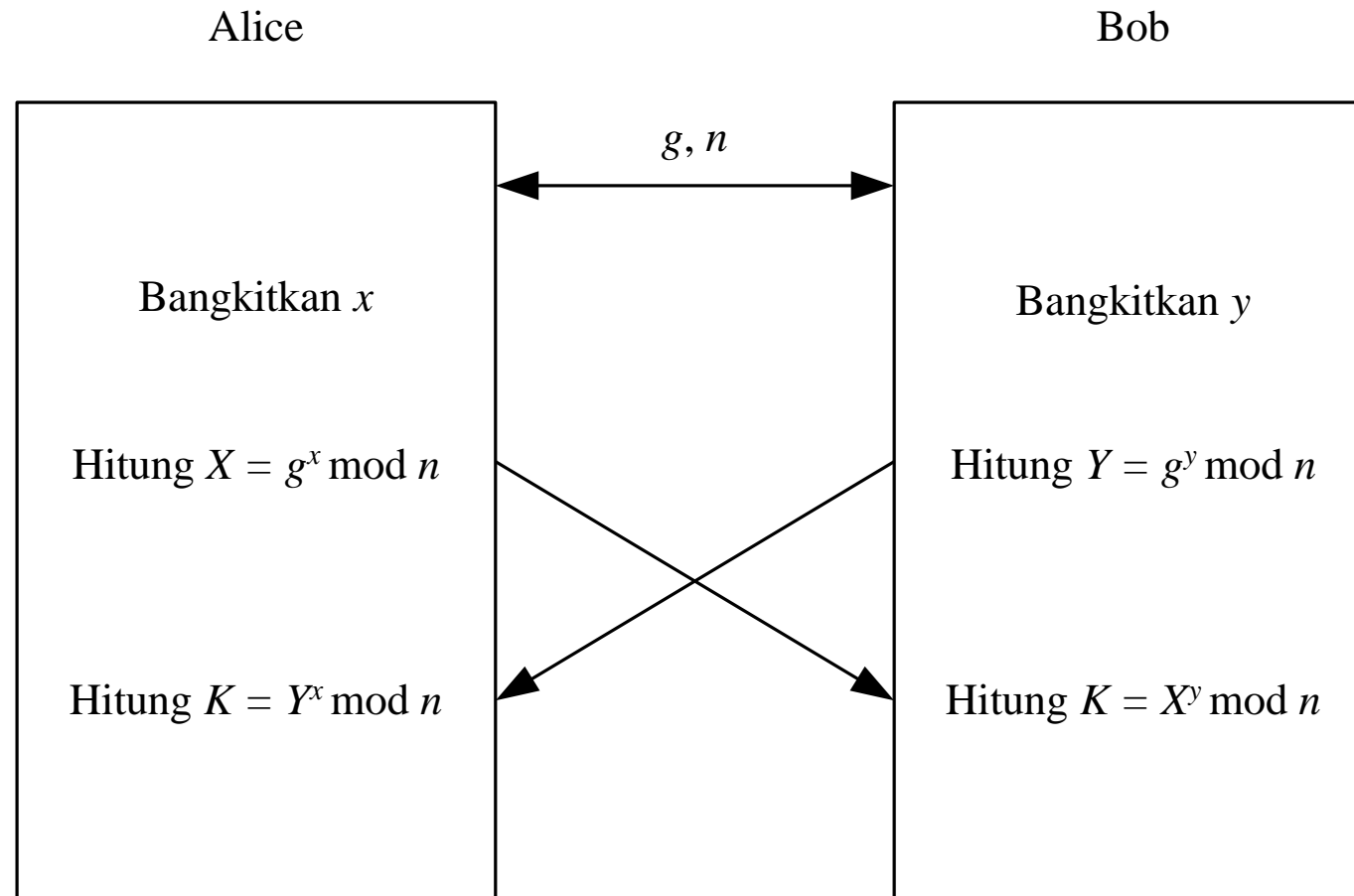
Bahan Kuliah II4031 Kriptografi dan Koding

- 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

# Elliptic Curve Diffie-Hellman (ECDH)

Ingatlah kembali diagram pertukaran kunci Diffie-Hellman:

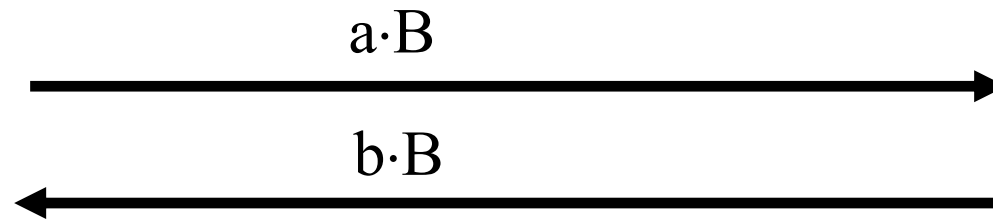


# Elliptic Curve Diffie-Hellman (ECDH)

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



Alice,  $A$



Bob,  $B$

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

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

Bahan Kuliah II4031 Kriptografi dan Koding

## Algoritma Elliptic Curve Diffie-Hellman (ECDH)

- Alice dan Bob ingin berbagi sebuah kunci rahasia  $K$  yang sama.
  - Alice dan Bob menyepakati kurva eliptik  $y^2 = x^3 + ax + b \pmod p$  dan titik  $B$  pada kurva
  - 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  $\rightarrow K_{AB} = a \cdot P_B = a \cdot (b \cdot B)$
    - Bob  $\rightarrow K_{AB} = b \cdot P_A = b \cdot (a \cdot B)$
    - **Kunci rahasia =  $K_{AB} = abB$**

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

$$K_B = b \cdot P_A = 3Q = Q + Q + Q = (0, 4)$$

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

# Elliptic Curve Elgamal (ECEG)

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



- Alice memilih bilangan acak  $k$  yang harus terletak di dalam selang  $[1, p-1]$
  - Cipherteks dari  $P_M$  adalah pasangan titik
    - $P_C = [ (kB), (P_M + kP_B) ]$
- 

- Untuk mendekripsi, Bob mula-mula menghitung hasil kali titik pertama dari  $P_C$  (yaitu  $kB$ ) 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 Elgamal dengan Elliptic Curve Elgamal

- Cipherteks pada EC-Elgamal adalah pasangan titik
    - $P_C = [ (kB), (P_M + kP_B) ]$  (ket:  $P_b =$  kunci publik Bob)
  - Cipherteks pada Elgamal juga pasangan nilai:
    - $C = (g^k \bmod p, my_B^k \bmod p)$  (ket:  $y_b =$  kunci publik Bob)
- 
- Pada EC\_Elgamal, Bob mengurangkan titik kedua dari  $P_C$  dengan hasil kali  $b \cdot (kB)$ 
    - $(P_M + kP_B) - [b(kB)] = P_M + k(bB) - b(kB) = P_M$
  - Pada El Gamal, Bob membagi nilai kedua dengan nilai pertama yang dipangkatkan dengan kunci privat Bob
    - $m = my_B^k / (g^k)^b = mg^{k*b} / g^{k*b} = m$

# *Encoding* Pesan menjadi Titik di dalam Kurva

- Pesan yang akan dienkripsi dengan ECC harus dikonversi (*encoding*) menjadi titik di dalam kurva eliptik.
- Metode yang sederhana adalah memetakan setiap karakter ASCII dengan setiap titik pada kurva eliptik.
- Untuk 256 karakter ASCII, maka dibutuhkan kurva eliptik yang berisi minimal 256 titik.
- Misalkan pesan  $M = \text{'ENCRYPT'}$ , yang dalam nilai ASCII adalah '69' '78', '67', '82', '89', '80', '84'. Setiap nilai ini dipetakan ke sebuah titik pada kurva eliptik.
- Namun metode ini kurang aman.

- Metode kedua adalah dengan metode Kolbitz. Langkah-langkahnya adalah sebagai berikut:
  1. Pilih sebuah kurva eliptik  $y^2 = x^3 + ax + b \pmod p$  yang mengandung  $N$  buah titik.
  2. Misalkan karakter-karakter penyusun pesan adalah angka 0, 1, 2, ..., 9 dan huruf A, B, C, ... Z yang dikodekan menjadi 10, 11, ..., 35.
  3. Kodekan setiap karakter di dalam pesan menjadi nilai  $m$  di antara 0 dan 35.
  4. Pilih sebuah bilangan bulat  $k$  sebagai parameter basis (disepakati kedua pihak).
  5. Untuk setiap nilai  $mk$ , nyatakan  $x = mk + 1$ , sulihkan  $x$  ke dalam  $y^2 = x^3 + ax + b \pmod p$  lalu tentukan nilai  $y$  yang memenuhi.
  6. Jika tidak ada nilai  $y$  yang memenuhi, coba untuk  $x = mk + 2$ ,  $x = mk + 3$ , dst, sampai  $y^2 = x^3 + ax + b \pmod p$  dapat dipecahkan.
  7. Pada proses *decoding*, untuk titik  $(x, y)$ , tentukan nilai  $m$  terbesar tetapi lebih kecil dari  $(x - 1)/k$ . Kodekan titik  $(x, y)$  menjadi symbol  $m$ .

**Contoh:** Misalkan  $y^2 = x^3 - x + 188 \pmod{751}$ . Kurva eliptik ini memiliki  $N = 727$  buah titik.

- Misalkan karakter yang akan dikodekan adalah huruf 'B', yang dikodekan menjadi nilai 11.
- Pilih  $k = 20$ , maka  $x = mk + 1 = (11)(20) + 1 = 221$ . Sulihkan  $x = 221$  ke dalam kurva eliptik  $y^2 = x^3 - x + 188 \pmod{751} \equiv 456 \pmod{751}$ . Tidak ada nilai  $y$  yang memenuhi.
- Coba untuk  $x = mk + 2 = (11)(20) + 2 = 222$ . Sulihkan  $x = 222$  ke dalam kurva eliptik  $y^2 = x^3 - x + 188 \pmod{751}$ . Juga tidak ada nilai  $y$  yang memenuhi.
- Coba untuk untuk  $x = mk + 3 = (11)(20) + 3 = 223$ . Sulihkan  $x = 223$  ke dalam kurva eliptik  $y^2 = x^3 - x + 188 \pmod{751}$ . Juga tidak ada nilai  $y$  yang memenuhi.
- Coba untuk untuk  $x = mk + 4 = (11)(20) + 4 = 224$ . Sulihkan  $x = 224$  ke dalam kurva eliptik  $y^2 = x^3 - x + 188 \pmod{751}$ . Diperoleh  $y = 248$ . Jadi, karakter 'B' dikodekan menjadi titik  $(224, 248)$  pada kurva eliptik.
- Pada proses *decoding*, hitung  $m = \lfloor (x - 1)/k \rfloor = \lfloor (224 - 1)/20 \rfloor = \lfloor 11.15 \rfloor = 11$ . Jadi pesan semula adalah huruf 'B'.

# 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



TAMAT