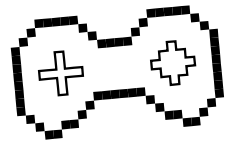
Praktikum Kriptografi

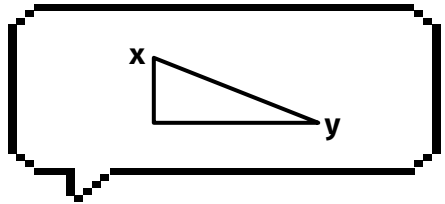
Pertemuan - 10

Topik: Elliptic Curve Cryptography (ECC)

Review



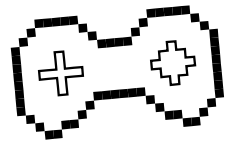
- **DES**
- **S-DES**



ECC

(Elliptic Curve Cryptography)

Elliptic Curve Cryptography



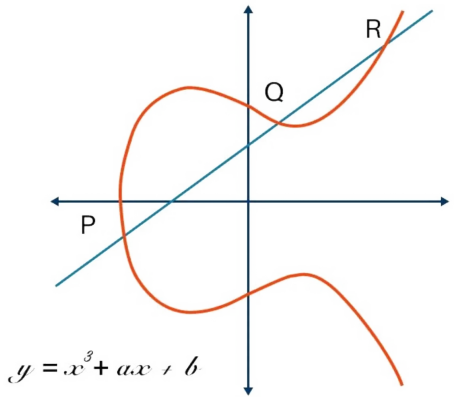
ECC merupakan sebuah pendekatan **public-key cryptography** yang memanfaatkan **struktur aljabar dari kurva eliptik** pada finite field.

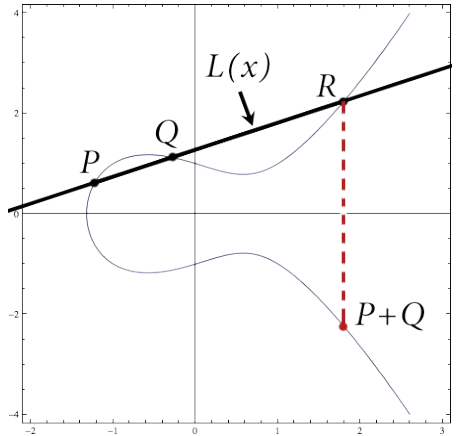
ECC memungkinkan **penggunaan key yang lebih kecil** dibanding algoritma public key lainnya, **untuk menyediakan tingkat keamanan yang setara**, sehingga dapat dikatakan bahwa algoritma ini **lebih kuat**.

"One of the most powerful, but least understood in use today"

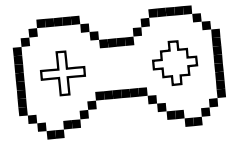
Visualisasi ECC

Visualisasi kurva eliptik bukan berbentuk elips atau oval, melainkan **garis lingkaran yang memotong dua sumbu** (garis pada grafik yang digunakan **untuk menunjukkan posisi suatu titik**).



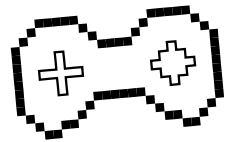


Aplikasi ECC



- Key Agreement
- Digital Signature
- Pseudo-random Generator
- Encryption
- Dasar Integer Factorization Algorithms

Bentuk Umum



ECC secara umum memiliki **bentuk** seperti berikut:

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

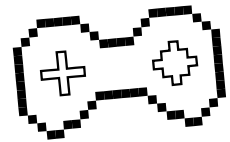
Dimana **p** merupakan **bilangan prima lebih besar dari 3**:

{p > 3, p ∈ bilangan prima}

Kriteria Euler: **R** merupakan **Quadratic Residue (QR)** jika:

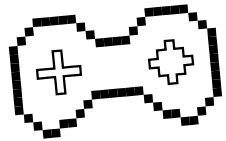
$$R^{(p-1)/2} \equiv 1 \pmod{p}$$

Step-by-Step



- Tentukan nilai ***p*, *a*,** dan ***b*** dari ECC
- Ambil **plaintext (Pt)** yang akan dienkripsi **(p_1,p_2)**
- Tentukan sembarang **titik *α*** pada kurva sebagai **titik “pembangkit”**
- Tentukan konstanta ***q* untuk enkripsi** dan ***r* untuk dekripsi**
- **$E(p_1,p_2) = (y_1,y_2)$,** dimana :
  - **$y_1 = q\alpha$**
  - **$y_2 = (p_1,p_2) + q.(r\alpha)$**
- **$D(y_1,y_2) = y_2 - (r.y_1)$**

Aturan ECC



$$Misalkan \begin{cases} P = (x_1, y_1) \\ Q = (x_2, y_2) \end{cases} \quad Jika \quad \left.\begin{matrix} x_1 = x_2 \\ y_1 = -y_2 \end{matrix}\right\rangle \; P + Q = 0$$

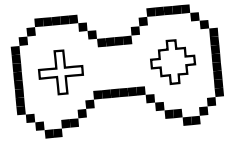
$$P + Q = \begin{cases} x_3 = \lambda^2 - x_1 - x_2 \\ y_3 = \lambda(x_1 - x_3) - y_1 \end{cases}$$

$$\lambda = \begin{cases} \dfrac{y_2 - y_1}{x_2 - x_1}, & utk \;\; P \neq Q \\ \dfrac{3{x_1}^2 + a}{2y_1}, & utk \;\; P = Q \end{cases}$$

-(x, y) = (x, -y)

P + Q = (x_3, y_3)

Contoh Soal



Misalkan **p = 11, a = 1** dan **b = 6** sehingga didapat kurva elips:

$y^2 \equiv x^3 + x + 6 \pmod{11}$, E = 14

Konstanta yang merupakan ***Quadratic Residue*** **(QR)** modulo 11 adalah:

1, 3, 4, 5, 9

$$1^5 \equiv 1 \pmod{11} \quad 3^5 \equiv 1 \pmod{11}$$
$$4^5 \equiv 1 \pmod{11} \quad 5^5 \equiv 1 \pmod{11}$$
$$9^5 \equiv 1 \pmod{11}$$

Contoh Soal

Mencari **nilai y** yang memungkinkan:

$$1^2 = 1 \pmod{11}$$

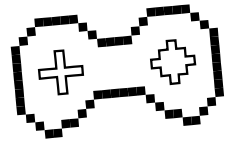
$$4^2 = 5 \pmod{11} \qquad 7^2 = 5 \pmod{11}$$

$$5^2 = 3 \pmod{11} \qquad 6^2 = 3 \pmod{11}$$

$$2^2 = 4 \pmod{11} \qquad 9^2 = 4 \pmod{11}$$

$$3^2 = 9 \pmod{11} \qquad 8^2 = 9 \pmod{11}$$

Contoh Soal

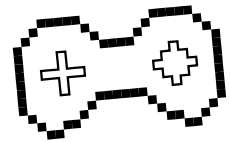


Tabel dari nilai x terhadap fungsi ECC yang memenuhi nilai **QR** dan **y** :

x	$x^3 + x + 6$	mod 11	$R^{(p-1)/2} \equiv 1 \bmod p$	QR(11)	y
2	16	5	1	yes	(4,7)
3	36	3	1	yes	(5,6)
5	136	4	1	yes	(2,9)
7	356	4	1	yes	(2,9)
8	526	9	1	yes	(3,8)

Note: Dalam proses pengerjaan soal, seluruh nilai x harus dihitung QR dan y-nya, contoh tabel ini disimplifikasi untuk QR yang memenuhi saja agar lebih efisien.

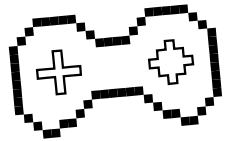
Contoh Soal



Nilai α yang memungkinkan dari tabel :

- y = 6 → (3,6)
- y = 7 → (2,7)
- y = 8 → (8,8)
- y = 9 → (5,9), (7,9)

Contoh Soal



Dengan menggunakan informasi yang didapatkan sebelumnya, enkripsikan **plaintext (Pt) = (10,9)** dengan fungsi pembangkit ***α* = (2,7).** Gunakan konstanta enkripsi **q = 3** dan konstanta dekripsi **r = 7.**

Step 1: Cari nilai β = q*α*

$$\alpha + \alpha = (2,7) + (2,7)$$

$$\lambda = \frac{3x_1^{\,2} + a}{2y_1} = \frac{3.4+1}{2.7} = \frac{13}{14} \pmod{11}$$

$$= 13.4 \pmod{11} = 8 \pmod{11}$$

$$x_3 = \lambda^2 - x_1 - x_2 = 64 - 2 - 2$$

$$= 60 \pmod{11} = 5 \pmod{11}$$

$$y_3 = \lambda(x_1 - x_3) - y_1 = 8(2-5) - 7$$

$$= -31 \pmod{11} = 2 \pmod{11}$$

$$\therefore 2\alpha = (5,2)$$

$$2\alpha + \alpha = (5,2) + (2,7)$$

$$\lambda = \frac{y_2 - y_1}{x_2 - x_1} = \frac{7-2}{2-5} = \frac{5}{-3} \pmod{11}$$

$$= 5.-4 \pmod{11} = 2 \pmod{11}$$

$$x_3 = \lambda^2 - x_1 - x_2 = 4 - 5 - 2$$

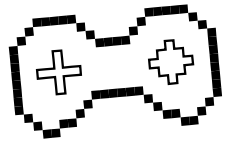
$$= -3 \pmod{11} = 8 \pmod{11}$$

$$y_3 = \lambda(x_1 - x_3) - y_1 = 2(5-8) - 2$$

$$= -8 \pmod{11} = 3 \pmod{11}$$

$$\therefore 3\alpha = (8,3)$$

Contoh Soal



Enkripsi :

$y_1 = q\alpha$

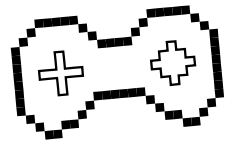
$y_2 = (p_1, p_2) + q.(r\alpha)$

$$y_1 = 3.\alpha = 3(2,7) = (8,3)$$

$$y_2 = (p_1, p_2) + 3(7.\alpha) = (10,9) + 3(7,2)$$
$$= (10,9) + (3,5) = (10,2)$$

$$\therefore \textit{Hasil Enkripsi adalah } \{(8,3),(10,2)\}$$

Contoh Soal



Dekripsi :

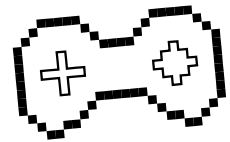
$$(p_1, p_2) = y_2 - r.y_1$$

$$= (10,2) - 7(8,3) = (10,2) - (3,5) = (10,2) + (3,-5) \mid -5 \bmod 11$$

$$= (10,2) + (3,6) = (10,9)$$

Hasil dekripsi: **(10,9)**

Note Singkat

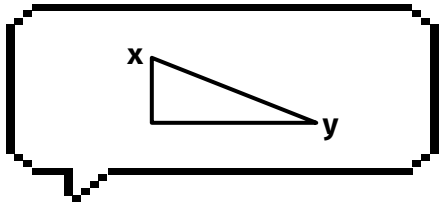


Kecuali disebutkan secara eksplisit pada permasalahan,

Nilai p persamaan ECC, biasanya **nilai prima terakhir dari satu siklus ECC**, misal:

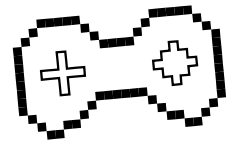
$$E = 34$$

Maka persamaan akan memiliki **nilai p** dengan bilangan prima **31.**



Tugas

Tugas 1



Misalkan diberikan persamaan **ECC**, sebagai berikut :

$y^2 \equiv x^3 + x + 13 \ (mod\ 31)$

$p = 31$

$a = 1$

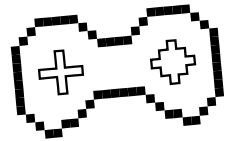
$b = 13$

Jumlah E = 34, Element ke-34 di E = (9, 10)

Buatlah dan Carilah :

- **Tabel** untuk menghitung **seluruh nilai QR** dan **y** untuk **setiap x yang ada** (seperti pada slide 12)
- Seluruh **nilai y** dan α yang memungkinkan
- Misalkan $\beta = a\alpha$, dimana **a = 25**, dengan menggunakan fungsi pembangkit α **= (9,10)**, carilah nilai β. (**Tampilkan fungsi yang digunakan hingga mendapat 7α, selebihnya silahkan menggunakan tabel untuk simplifikasi jika dibutuhkan**).

Tugas 2



Misalkan diberikan persamaan **ECC**, sebagai berikut :

$y^2 \equiv x^3 + x + 6 \ (mod\ 31)$

$p = 31$

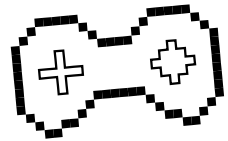
$a = 1$

$b = 6$

Lakukan :

- **Enkripsi:**
  - **Plaintext: (7,8)**
  - α **= (3,6)**
  - **q = 2**
- **Dekripsi:**
  - **Gunakan Ciphertext yang didapatkan dari proses enkripsi**
  - **r = 3**

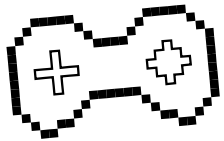
Tugas



Kumpulkan Tugas 1 dan Tugas 2 dalam 1 file PDF di Google Classroom, dengan format :

Format: Tugas10_NPM.pdf

Deadline Tugas: H-1 Praktikum Berikutnya, 23.59



Thank You!!

Kalau misalkan ada pertanyaan,
yaudah tanya aja

Praktikum Kriptografi 2022