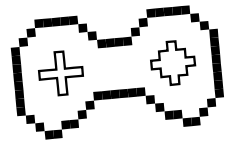
Praktikum Kriptografi

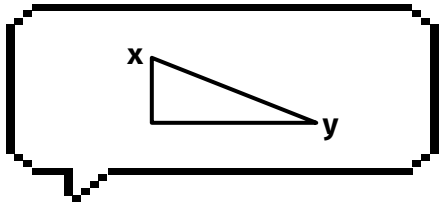
Pertemuan - 11

Menezez-Vanstone ECC

Review

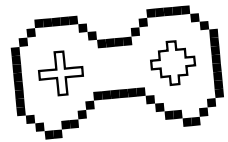


- **ECC**



Menezez-Vanstone ECC

Menezez-Vanstone ECC

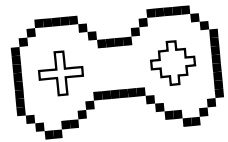


Menezez-Vanstone Elliptic Curve merupakan pengembangan dari algoritma ECC sebelumnya. Di mana algoritma ini merupakan salah satu solusi untuk memecahkan permasalahan *encoding* di suatu titik.

Perbedaan algoritma Menezez-Vanstone dengan Elliptic Curve yang biasanya terletak pada pesan yang akan dienkripsinya.

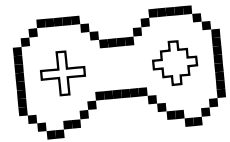
Jika pada ECC pesan diletakan pada titik di kurva eliptik, sedangkan pada Menezez-Vanstone ECC pesan yang akan dienkripsi **disamarkan** sehingga hasil enkripsinya akan menghasilkan tiga titik yaitu **y0, y1, y2**

Algoritma



1. Tentukan nilai **p, a, b** untuk membuat kurva eliptik
2. Misalkan plainteks yang akan di enkripsi **(p1, p2)**
3. Tentukan sebarang titik **α** pada kurva sebagai **titik pembangkit**
4. Tentukan konstanta **q** untuk **enkripsi** dan **r** untuk **dekripsi**

Enkripsi



Rumus untuk enkripsi:

E(p1, p2) = (y0, y1, y2) dimana :

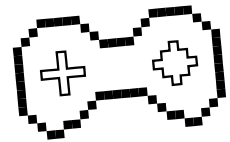
y0 = qα

(c1, c2) = q(r.α)

y1 = c1 . p1 (mod p)

y2 = c2 . p2 (mod p)

Dekripsi



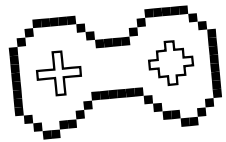
Rumus untuk dekripsi:

1. Tentukan terlebih dahulu **(c1, c2) = r . y0**
2. **D(y0, y1, y2)** = **(p1, p2)**

$$p1 = y_1 c_1^{-1} \bmod p$$

$$p2 = y_2 c_2^{-1} \bmod p$$

Contoh Soal Enkripsi



Misalkan **plainteks = (9, 1)**, fungsi pembangkit **α = (2, 7)**
Konstanta enkripsi **q = 6** dan konstanta deskripsi **r = 7**

- **Enkripsi:**

$$y_0 = 6.\alpha = 6(2,7) = (7,9)$$

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

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

$$= 13.4(\text{mod } 11) = 8(\text{mod } 11)$$

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

$$= 60(\text{mod } 11) = 5(\text{mod } 11)$$

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

$$= -31(\text{mod } 11) = 2(\text{mod } 11)$$

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

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

$$\lambda = \frac{y_2 - y_1}{x_2 - x_1} = \frac{7-2}{2-5} = \frac{5}{-3} (\text{mod } 11)$$

$$= 5.-4(\text{mod } 11) = 2(\text{mod } 11)$$

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

$$= -3(\text{mod } 11) = 8(\text{mod } 11)$$

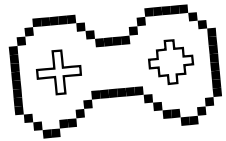
$$y_3 = \lambda(x_1 - x_3) - y_1 = 2(5-8) - 2$$

$$= -8(\text{mod } 11) = 3(\text{mod } 11)$$

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

$4\alpha = (10,2)$; $5\alpha = (3,6)$; $6\alpha = (7,9)$

Contoh Soal Enkripsi



Ulangi proses di atas hingga didapat $\beta = 7.\alpha = (7,2)$

$x = (x_1,x_2) = (9,1)$; $k = 6$, sehingga dapat dihitung

$y_0 = k\alpha = 6.(2,7) = (7,9)$

$(c_1,c_2) = k\beta = 6.(7,2) = (8,3)$

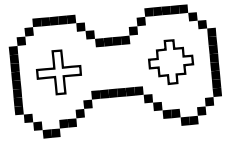
Sehingga didapat nilai $c_1 = 8$ dan $c_2 = 3$

$y_1 = c_1x_1 \bmod p = 8 \times 9 \bmod 11 = 6$

$y_2 = c_2x_2 \bmod p = 3 \times 1 \bmod 11 = 3$

$\therefore$ *Hasil Enkripsi adalah* $\{(7,9),6,3\}$

Contoh Soal Dekripsi



- **Dekripsi:**

$$(c_1, c_2) = r.y_0 = 7(7,9) = (8,3)$$

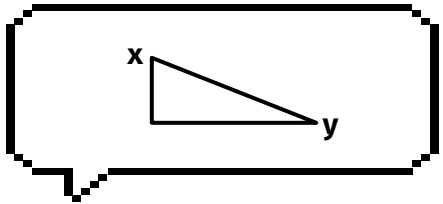
$$(p_1, p_2) = \left(y_1 c_1^{-1} \bmod p \ , \ y_2 c_2^{-1} \bmod p\right)$$

$$= \left(6.8^{-1} \bmod 11 \ , \ 3.3^{-1} \bmod 11\right)$$

$$= (6.7 \bmod 11 \ , 3.4 \bmod 11)$$

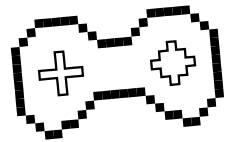
$$= (9,1)$$

Hasil dekripsi: **(9, 1)**



Tugas

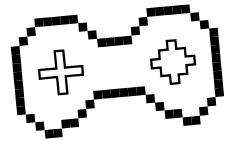
Tugas



Misalkan **p = 31, a = 1** dan **b = 6** sehingga didapat kurva elips:
$\mathbf{y^2 \equiv x^3 + x + 6 \ (\ mod \ 31 \ )}$

Lakukan proses **enkripsi** dan **dekripsi** menggunakan kriptografi **kurva elips Menezes-Vanstone** untuk plainteks = **(7, 8)** dan fungsi pembangkit
α = (3, 6) dengan **q = 2 dan r = 3.**

Tugas



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

Format: Tugas11_NPM.pdf

Deadline Tugas: H-1 Praktikum Berikutnya, 23.59

KUIS-2!!!