TUGAS 10

PRAKTIKUM KRIPTOGRAFI

Disusun oleh:

Muhamad Rumi Rifai - 140810220026

PROGRAM STUDI S-1 TEKNIK INFORMATIKA

FAKULTAS MATEMATIKA DAN ILMU PENGETAHUAN ALAM

UNIVERSITAS PADJADJARAN

JATINANGOR

2024

Soal

1. Misalkan **p = 31, a = 1,** dan **b = 6** sehingga didapat kurva elips:
   $y^2 \equiv x^3 + x + 6 \ (mod\ 31)$
   Lakukan proses **enkripsi** dan **dekripsi** menggunakan kriptografi **kurva elips Menezes-Vanstone** untuk plaintext = **(7,8)** dan fungsi pembangkit **α = (3,6)** dengan **q = 2** dan **r = 3**

Jawab

- **Enkripsi**
  - $y_0 = qa = 2a$
    $2a = a + a = (3,6) + (3,6)$
    $\lambda = \frac{3x_1^2+a}{2y_1} = \frac{3*9+1}{2*6} = \frac{28}{12} \bmod 31 = 364 \bmod 31 = 23$
    $x_3 = \lambda^2 - x_1 - x_2 = 23^2 - 9 - 9 = 523 \bmod 31 = 27$
    $y_3 = \lambda\,(x_1 - x_3) - y_1 = 23(3-17) - 6 = -558 \bmod 31 = 0$
    $2a = (27,0)$
  - $3a = 2a + a = (27,0) + (3,6)$
    $\lambda = \frac{y_2+y_1}{x_2+x_1} = \frac{6-0}{3-27} = \frac{6}{-24} \bmod 31 = 54 \bmod 31 = 23$
    $x_3 = \lambda^2 - x_1 - x_2 = 23^2 - 27 - 3 = 499 \bmod 31 = 3$
    $y_3 = \lambda\,(x_1 - x_3) - y_1 = 23(27-3) - 0 = 552 \bmod 31 = 25$
    $3a = (3,25)$
  - $6a = 3a + 3a = (3,25) + (3,25)$
    $\lambda = \frac{3x_1^2+a}{2y_1} = \frac{3*9+1}{2*25} = \frac{28}{19} \bmod 31 = 504 \bmod 31 = 8$
    $x_3 = \lambda^2 - x_1 - x_2 = 8^2 - 3 - 3 = 27 \bmod 31 = 27$
    $y_3 = \lambda\,(x_1 - x_3) - y_1 = 8(3-27) - 25 = 217 \bmod 31 = 0$
    $6a = (c_1, c_2) = (27,0)$
  - $y_1 = c_1 * p_1 \bmod p = 27*7 \bmod 31 = 3$
    $y_2 = c_2 * p_2 \bmod p = 0*8 \bmod 31 = 0$
    Maka hasil dari enkripsi plaintext adalah {(27,0),(3,0)}

- **Dekripsi**
  - $(c_1, c_2) = r * y_0 = 3(27,0)$

    $2a = a + a = (27,0) + (27,0)$

    $\lambda = \frac{3x_1^2+a}{2y_1} = \frac{3*27+1}{2*0} = \frac{2188}{0} \bmod 31 = 0 \bmod 31 = 0$

    $x_3 = \lambda^2 - x_1 - x_2 = 0^2 - 27 - 27 = -54 \bmod 31 = 8$

    $y_3 = \lambda (x_1 - x_3) - y_1 = 0(27-8) - 0 = 0 \bmod 31 = 0$

    $2a = (8,0)$
  - $3a = 2a + a = (8,0) + (27,0)$

    $\lambda = \frac{y_2+y_1}{x_2+x_1} = \frac{0-0}{27-8} = \frac{0}{19} \bmod 31 = 0 \bmod 31 = 0$

    $x_3 = \lambda^2 - x_1 - x_2 = 0^2 - 8 - 27 = -35 \bmod 31 = 27$

    $y_3 = \lambda (x_1 - x_3) - y_1 = 0(8-27) - 0 = 0 \bmod 31 = 0$

    $3a = (c_1, c_2) = (27,0)$
  - $y_1 = c_1 * p_1 \bmod p = 3*23 \bmod 31 = 7$

    $y_2 = c_2 * p_2 \bmod p = 0*0 \bmod 31 = 0$

    Maka hasil dari enkripsi plaintext adalah {(7,0)}