Nama : Prames Ray Lapian
NPM : 140810210059

Soal:

Misalkan p = 31, a = 1 dan b = 6 sehingga didapat kurva elips: y2 ≡ x3 + 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.

Jawaban:

Enkripsi:

Menghitung y0:

$y0 = q \cdot \alpha$
= 2(3, 6)
2α = α + α
= (3, 6) + (3, 6)
λ = (3x1 2 + a) (2y1)−1 mod 31
= 3(3)2 + 1)(2(6))−1 mod 31
= (3(9) + 1)(12)−1 mod 31
= (3(9) + 1)(13)mod 31
= 28(13)mod 31
= 364 mod 31
= 23

x3 = (λ2 − x1 − x2) mod 31
x3 = (232 − 3 − 3) mod 31
x3 = (529 − 6) mod 31
x3 = 27

y3 = (λ(x1 − x3( ) − y1)mod 31
y3 = (23(3 − 27) − 6) mod 31
y3 = (− 558) mod 31
y3 = 0
Maka didapat y0 = 2α = (27, 0)

Menghitung rα yang dapat didefinisikan menjadi β, dimana β = 3α. 3α = 2α + α = (27, 0) + (3, 6)
λ = (y2 − y1) (x2 − x1) −1 mod 31
= (6 − 0)(3 − 27) −1 mod 31
= (6)(− 24) −1 mod 31
= (6)(7)−1 mod 31
= (6)(9) mod 31
= 54 mod 31
= 23

x3 = (λ2 – x1 – x2) mod 31
= (232 − 27 − 3) mod 31
= (529 − 30) mod 31
= 3

y3 = (λ (x1 − x3)−y1) mod 31
= (23(27 − 3) − 0) mod 31
= (552 − 0) mod 31
= 25

Maka β = 3α = (3, 25)

Menghitung (c1, c2) = q * β = 2(3, 25)
2β = β + β = (3, 25) + (3, 25)
λ = (3x1 2 + a) (2y1)−1 mod 31
= 3(3)2 + 1)(2(25))−1 mod 31
= (3(9) + 1)(19)−1 mod 31
= (3(9) + 1)(18)mod 31
= 28(18) mod 31
= 504 mod 31
= 8

x3 = (λ2 − x1 − x2) mod 31
= (82 − 3 − 3) mod 31
= (64 − 6) mod 31
= 27

y3 = (λ (x1 − x3)−y1) mod 31
= (8(3 − 27) − 25) mod 31
= (-217) mod 31
= 0

Maka didapat (c1, c2) = 2β = (27, 0)

Menghitung y1 dan y2

y1 = c1x1 mod 31
= 27(7) mod 31
= 189 mod 31
= 3

y2 = c2x2 mod 31
= 0(8) mod 31
= 0 mod 31
= 0

Jadi didapat ciphertext y = (y0, y1, y2) = ((27, 0), 3, 0).

Dekripsi:

Menghitung (c1, c2) = r * y0 = 2(3, 25)
(c1, c2) = 3(27, 0).

2α = α + α
= (27, 0) + (27, 0)

λ = (3x1 2 + a) (2y1)−1 mod 31
= 3(27)2 + 1)(2(0))−1 mod 31
= (3(729) + 1)(0)−1 mod 31
= (2187 + 1)(0)mod 31
= 2188(0) mod 31
= 0 mod 31
= 0

y3 = (λ (x1 − x3)−y1) mod 31
= (0(27 − 8) − 0) mod 31
= (0) mod 31
= 0

Maka didapat 2α = (8, 0)

3α = 2α + α
= (8, 0) + (27, 0)

λ = (y2 − y1) (x2 − x1)−1 mod 31
= (0 − 0)(27 − 8)−1 mod 31
= (0)(19)−1 mod 31
= (0)(18) mod 31
= 0 mod 31
= 0

x3 = (λ2 − x1 − x2) mod 31
= (02 − 8 − 27) mod 31
= -35 mod 31
= 27

y3 = (λ (x1 − x3)−y1) mod 31
= (0(8 − 27) − 0) mod 31
= (0) mod 31
= 0

Maka didapat (c1, c2) = 3α = (27, 0)

Menghitung x sebagai berikut:
x = (y1c1−1 mod 31, y2c2−1 mod 31)

x1 = y1c1−1 mod 31
= 3(27)−1 mod 31
= 3(23) mod 31
= 69 mod 31
= 7

X2 = y2c2−1 mod 31
= 0(0)−1 mod 31
= 0(0) mod 31
= 0

Maka didapat plaintext x = (7, 0).