Nama : Prames Ray Lapian
NPM : 140810210059

Soal:

1. Misalkan diberikan persamaan ECC, sebagai berikut :
   $y2 \equiv x3 + x + 13 \ (mod\ 31)$
   $p = 31$
   $a = 1$
   $b = 13$
   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 β = aα, 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).

2. Misalkan diberikan persamaan ECC, sebagai berikut :
   y2 ≡ x3 + 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

Jawaban:

1. Cari konstanta yang Quadratic Residue pada P :

X	$x^3 + x + 13$	mod 31	R(p-1)/2 ≡ 1 mod p	QR(31)	y
2	23	23	30	no	
3	43	12	30	no	
4	81	19	1	Yes	(9, 22)
5	143	19	1	Yes	(9, 22)
6	235	18	1	Yes	(7, 24)
7	363	22	30	no	
8	533	6	30	no	
9	751	7	1	Yes	(10, 21)
10	1023	0	0	no	
11	1355	22	30	no	
12	1753	17	30	no	
13	2223	22	30	no	
14	2771	12	30	no	
15	3403	24	30	no	
16	4125	2	1	Yes	(8, 23)
17	4943	14	1	Yes	(13, 18)
18	5863	4	1	Yes	(2, 29)
19	6891	9	1	Yes	(3, 28)
20	8033	4	1	Yes	(2, 29)

21	9295	26	30	no	
22	10683	19	1	Yes	(9, 22)
23	12203	20	1	Yes	(12, 19)
24	13861	4	1	Yes	(2, 29)
25	15663	8	1	Yes	(15, 16)
26	17615	7	1	Yes	(10, 21)
27	19723	7	1	Yes	(10, 21)
28	21993	14	1	Yes	(13, 18)
29	24431	3	30	no	
30	27043	11	30	no	
31	29835	13	30	no	

Tabel untuk menghitung seluruh QR dan y untuk setiap X:

QR	**y**	
1	1	30
2	8	23
4	2	29
5	6	25
7	10	21
8	15	16
9	3	28
10	14	17
14	13	18
16	4	27

18	7	24
19	9	22
20	12	19
25	5	26
28	11	20

Seluruh nilai y dan α yang memungkinkan:

y	**α**		
16	25, 16		
18	17, 18	28, 18	
19	23, 19		
21	9, 21	26, 21	27, 21
22	4, 22	5,22	22, 22
23	16, 21		
24	6, 24		
28	19, 28		
29	18, 29	20, 29	24, 29

Cari β = aα dengan a = 25 dengan menggunakan fungsi pembangkit α = (9,10)

$$2a = a + a$$
$$= (9, 10) + (9, 10)$$

$$\lambda = \frac{3x_1^2 + a}{2y_1}$$
$$= \frac{3 \times 81 + 1}{2 \times 10}$$
$$= \frac{244}{20} (mod\ 31)$$
$$= 6\ (mod\ 31)$$

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

$= 36 - 9 - 9$

$= 18 \pmod{31}$

$= 18$

$y^3 = \lambda(x_1 - x_3) - y_1$

$= 6(9 - 18) - 10$

$= -64 \pmod{31}$

$= 29$

Jadi 2*a* = (18, 29)

$3a = 2a + a$

$= (18, 29) + (9, 10)$

$\lambda = \frac{y_2 + y_1}{x_2 + x_1}$

$= \frac{10 - 29}{9 - 18}$

$= \frac{-19}{-9} (mod\ 31)$

$= 9\ (mod\ 31)$

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

$= 81 - 18 - 9$

$= 54 \pmod{31}$

$= 23$

y3 = λ(x1 – x3) – y1
= 9(18 – 23) – 29
= -74 (mod 31)
= 19

Jadi 3a = (23, 19)

4a = 3a + a
= (23, 19) + (9, 10)

$\lambda = \frac{y_2+y_1}{x_2+x_1}$

$= \frac{10-29}{9-23}$

$= \frac{-9}{-14}(mod\ 31)$

$= 25\ (mod\ 31)$

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

= 625 – 23 – 9

= 593 (mod 31)

= 4

$y_3 = \lambda(x_1 - x_3) - y_1$

= 25(23 – 4) – 19

= 456 (mod 31)

= 22

Jadi 4a = (4, 22)

5a = 4a + a

= (4, 22) + (9, 10)

$\lambda = \frac{y_2+y_1}{x_2+x_1}$

$= \frac{10-22}{9-4}$

$= \frac{-12}{5}(mod\ 31)$

$= \ 10\ (mod\ 31)$

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

$= 100 - 4 - 9$

$= 87 \pmod{31}$

$= 25$

$y_3 = \lambda(x_1 - x_3) - y_1$

$= 10(4 - 25) - 22$

$= -232 \pmod{31}$

$= 16$

Jadi 5a = (25, 16)

$6a = 5a + a$

$= (25, 16) + (9, 10)$

$\lambda = \frac{y_2+y_1}{x_2+x_1}$

$= \frac{10-16}{9-25}$

$= \frac{-6}{-16}(mod\ 31)$

$= \ 12\ (mod\ 31)$

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

$= 144 - 25 - 9$

$= 110 \pmod{31}$

$= 17$

$y_3 = \lambda(x_1 - x_3) - y_1$

$= 12(25 - 17) - 16$

$= 80 \pmod{31}$

$= 18$

Jadi 6a = (17, 18)

7a $= 6a + ad$

$= (17, 18) + (9, 10)$

$\lambda = \frac{y_2 + y_1}{x_2 + x_1}$

$= \frac{10-18}{9-17}$

$= \frac{-8}{-8} (mod\ 31)$

$= 1\ (mod\ 31)$

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

$= 1 - 17 - 9$

$= -25 \pmod{31}$

$= 6$

$y_3 = \lambda(x_1 - x_3) - y_1$

$= 1(17 - 6) - 18$

$= -7 \pmod{31}$

$= 24$

Jadi 7a = (6, 24)

2. Mencari konstanta yang quadratic residue modulo 31:

$1^{15} \equiv 1 \pmod{31}$
$2^{15} \equiv 1 \pmod{31}$
$4^{15} \equiv 1 \pmod{31}$
$5^{15} \equiv 1 \pmod{31}$
$7^{15} \equiv 1 \pmod{31}$
$8^{15} \equiv 1 \pmod{31}$
$9^{15} \equiv 1 \pmod{31}$
$10^{15} \equiv 1 \pmod{31}$
$14^{15} \equiv 1 \pmod{31}$
$16^{15} \equiv 1 \pmod{31}$
$18^{15} \equiv 1 \pmod{31}$
$19^{15} \equiv 1 \pmod{31}$
$20^{15} \equiv 1 \pmod{31}$
$25^{15} \equiv 1 \pmod{31}$
$28^{15} \equiv 1 \pmod{31}$

Mencari nilai y yang memungkinkan :

$2^2 \equiv 4 \pmod{31}$
$3^2 \equiv 9 \pmod{31}$
$4^2 \equiv 16 \pmod{31}$
$5^2 \equiv 25 \pmod{31}$
$6^2 \equiv 6 \pmod{31}$
$7^2 \equiv 18 \pmod{31}$
$8^2 \equiv 2 \pmod{31}$
$9^2 \equiv 19 \pmod{31}$
$10^2 \equiv 7 \pmod{31}$
$11^2 \equiv 28 \pmod{31}$
$12^2 \equiv 20 \pmod{31}$
$13^2 \equiv 14 \pmod{31}$
$14^2 \equiv 10 \pmod{31}$
$15^2 \equiv 8 \pmod{31}$
$16^2 \equiv 8 \pmod{31}$
$17^2 \equiv 10 \pmod{31}$
$18^2 \equiv 14 \pmod{31}$
$19^2 \equiv 20 \pmod{31}$
$20^2 \equiv 28 \pmod{31}$
$21^2 \equiv 7 \pmod{31}$
$22^2 \equiv 19 \pmod{31}$
$23^2 \equiv 2 \pmod{31}$
$24^2 \equiv 18 \pmod{31}$
$25^2 \equiv 5 \pmod{31}$
$26^2 \equiv 25 \pmod{31}$
$27^2 \equiv 16 \pmod{31}$

$28^2 \equiv 9 \pmod{31}$
$29^2 \equiv 4 \pmod{31}$
$30^2 \equiv 1 \pmod{31}$

x	$y^2 \equiv x^3 + x + 6 \pmod{31}$	y
1	8	15,16
2	16	4,27
3	5	6,25
12	10	14,17
14	5	6,25
17	7	10,21
18	28	11,20
19	2	8,23
20	28	11,20
21	19	9,22
24	28	11,20
25	1	1,30
28	7	10,21
30	4	2,29

Enkripsi:

$2\alpha = (3, 6) + (3, 6)$
$\lambda = (3.\ 32 + 1)\ (2.\ 6) - 1 \bmod 31$
$= 28.\ 12 - 1 \bmod 31$
$= 28.\ 13 \bmod 31$
$= 23$
$x1 = 23^2 - 3 - 3 \bmod 31$
$= 27$
$y1 = 23\ (3 - 27) - 6 \bmod 31$
$= 0$
$2\alpha = (27,0)$

3α = (27, 0) + (3, 6)
λ = (6 – 0) (3 − 27) − 1 mod 31
= 6. 9 mod 31
= 23
x2 = 23^2 − 27 − 3 mod 31
= 3
y2 = 23 (27 − 3) − 0 mod 31
= 25
3α = (3, 25)

6α = (3, 25) + (3, 25)
λ = (3. 252 + 1) (2. 27)-1 mod 31
= (3. 32 + 1) (2. 25) − 1 mod 31
= 28. 18 mod 31
= 8
x3 = 82 – 3 – 3 mod 31
= 27
y3 = 8 (3 − 27) – 25 mod 31
= 0
6α = (27, 0)

y2 = (7, 8) + (27, 0)
λ = (0 – 8)(27 − 7) − 1 mod 31
= − 8. 14 mod 31
= 12
x = 122 − 7 − 27 mod 31
= 17
y = 12 (7 − 17) − 8 mod 31
= 27
y2 = (17, 27)

y1 = 2α
= 2(3, 6)
= (27, 0)
y2 = (p1, p2) + q(rα)
= (7, 8) + 2(3α)
= (7, 8) + (27, 0)
= (17, 27)

Hasil dari enkripsi adalah {(27,0), (17,27)}

Dekripsi:
(p`, p2)= (17, 27) – 3(27, 0))
= (14 − 21)(16 − 9)-1 mod 31

= (17, 27) – 6α
= (17, 27) – (27, 0)

(p`, p2)= (17, 27) + (27, 0)
λ = (0 – 27) (27 − 17) − 1 mod 31
= − 27. 28 mod 31 = 19
x = 192– 17 − 27 mod 31
= 7
y = 19 (17 − 7) − 27 mod 31
= 8
(p1, p2) = (7, 8)

Hasil dari deskripsi adalah (7,8)