TUGAS 9

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 diberikan persamaan ECC, sebagai berikut :
   $y^2 \equiv x^3 + x + 13 \pmod{31}$
   $p = 31$
   $a = 1$
   $b = 13$
   Jumlah E = 34, Element ke-34 di E = (9, 10)
   Buatlah dan Carilah :
   a. Tabel untuk menghitung seluruh nilai QR dan y untuk setiap x yang ada (seperti pada slide 12)
   b. Seluruh nilai y dan α yang memungkinkan
   c. 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 :
   $y^2 \equiv x^3 + x + 6 \pmod{31}$
   $p = 31$
   $a = 1$
   $b = 6$
   Lakukan :
   a. Enkripsi:
      i. Plaintext: (7,8)
      ii. α = (3,6)
      iii. q = 2
   b. Dekripsi:
      i. Gunakan Ciphertext yang didapatkan dari proses enkripsi
      ii. r = 3

Jawab

1. Mencari konstanta yang quadratic residu 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	30	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	

Nilai 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

QR	y		
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)

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

  $x_3 = \lambda^2 - x_1 - x_2$ = 36-9-9 = 18 mod 31 = 18

  $y_3 = \lambda (x_1 - x_3) - y_1$ = 6(9-18)-10 =- 64 mod 31 = 29

  $2a$ = (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 = 53 mod 31 = 23

  $y_3 = \lambda (x_1 - x_3) - y_1$ = 9(18-23)-29 =- 74 mod 31 = 19

  $3a$ = (23,19)

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

  $\lambda = \frac{y_2+y_1}{x_2+x_1} = \frac{10-19}{9-23} = \frac{-9}{-14} \bmod 31 = 25 \bmod 31$

  $x_3 = \lambda^2-x_1-x_2 = 625-23-9 = 593 \bmod 31 = 4$

  $y_3 = \lambda (x_1-x_3)-y_1 = 25(23-4)-19 =- 456 \bmod 31 = 22$

  $4a = (4,22)$

- $5a = 4a + a = (4,22) + (9, 10)$

  $\lambda = \frac{y_2+y_1}{x_2+x_1} = \frac{10-22}{9-4} = \frac{-12}{5} \bmod 31 = 10 \bmod 31$

  $x_3 = \lambda^2-x_1-x_2 = 100-4-9 = 87 \bmod 31 = 25$

  $y_3 = \lambda (x_1-x_3)-y_1 = 10(4-25)-22 =- 32 \bmod 31 = 16$

  $5a = (25,16)$

- $6a = 5a + a = (25,16) + (9,10)$

  $\lambda = \frac{y_2+y_1}{x_2+x_1} = \frac{10-16}{9-25} = \frac{-6}{-16} \bmod 31 = 12 \bmod 31$

  $x_3 = \lambda^2-x_1-x_2 = 144-25-9 = 110 \bmod 31 = 17$

  $y_3 = \lambda (x_1-x_3)-y_1 = 12(25-17)-16 =- 80 \bmod 31 = 18$

  $6a = (17,18)$

- $7a = 6a + a = (17,18) + (9,10)$

  $\lambda = \frac{y_2+y_1}{x_2+x_1} = \frac{10-18}{9-17} = \frac{-8}{-8} \bmod 31 = 1 \bmod 31$

  $x_3 = \lambda^2-x_1-x_2 = 1-17-9 = 25 \bmod 31 = 6$

  $y_3 = \lambda (x_1-x_3)-y_1 = 1(17-6)-18 =- 7 \bmod 31 = 124$

  $7a = (6,24)$

2. Konstanta yang merupakan ***Quadratic Residue (QR)*** modulo 31 adalah:

$1^{15} \equiv 1 \ mod \ 31$

$2^{15} \equiv 1 \ mod \ 31$

$4^{15} \equiv 1 \ mod \ 31$

$5^{15} \equiv 1 \ mod \ 31$

$7^{15} \equiv 1 \ mod \ 31$

$8^{15} \equiv 1 \ mod \ 31$

$9^{15} \equiv 1 \ mod \ 31$

$10^{15} \equiv 1 \ mod \ 31$

$14^{15} \equiv 1 \ mod \ 31$

$16^{15} \equiv 1 \ mod \ 31$

$18^{15} \equiv 1 \ mod \ 31$

$19^{15} \equiv 1 \ mod \ 31$

$20^{15} \equiv 1 \ mod \ 31$

$25^{15} \equiv 1 \ mod \ 31$

$28^{15} \equiv 1 \ mod \ 31$

Mencari nilai y yang memungkinkan

Y	Y^2 mod 31
1	1
2	4
3	9
4	16
5	25
6	5
7	18
8	2
9	19
10	7

11	28
12	20
13	14
14	10
15	8
16	8
17	10
18	14
19	20
20	28
21	7
22	19
23	2
24	18
25	5
26	25
27	16
28	9
29	4
30	1

X	x^3+x+6	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	29	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:

- $2a = a + a = (3,6) + (3,6)$

  $\lambda = (3 * 32 + 1)(2 * 6)^{-1} \, mod \, 31 = 23$

  $x_3 = \lambda^2 - x_1 - x_2 = 23^2 - 3 - 3 \bmod 31 = 27$

  $y_3 = \lambda \, (x_1 - x_3) - y_1 = 23(3-27) - 6 \bmod 31 = 0$

  Maka didapat $2a = (27,0)$
- $3a = 2a + a = (27,0) + (3,6)$

  $\lambda = (6 - 0)(3 - 27)^{-1} \, mod \, 31 = 23$

  $x_3 = \lambda^2 - x_1 - x_2 = 23^2 - 27 - 3 \bmod 31 = 3$

  $y_3 = \lambda \, (x_1 - x_3) - y_1 = 23(27-3) - 0 \bmod 31 = 25$

  Maka didapat $3a = (3,25)$
- $6a = 3a + 3a = (3,25) + (3,25)$

  $\lambda = (3 * 25^2 + 1)(2 * 27)^{-1} \, mod \, 31 = 8$

  $x_3 = \lambda^2 - x_1 - x_2 = 8^2 - 3 - 3 \bmod 31 = 27$

  $y_3 = \lambda \, (x_1 - x_3) - y_1 = 8(3-27) - 25 \bmod 31 = 0$

  Maka didapat $6a = (27,0)$
- $y^2 = (7,8) + (27,0)$

  $\lambda = (0 - 8)(27 - 7)^{-1} \, mod \, 31 = 12$

  $x_3 = \lambda^2 - x_1 - x_2 = 12^2 - 7 - 27 \bmod 31 = 17$

  $y_3 = \lambda \, (x_1 - x_3) - y_1 = 12(7-17) - 8 \bmod 31 = 27$

Maka didapat y^2 = (17,27)

y_1 = 2a = 2(3,6) = (27,0)

y_2 = (p_1,p_2)+q(ra) = (7,8)+2(3) = (7,8)+(27,0) = (17,27)

Maka hasil dari enkripsi plaintext adalah {(27,0),(17,27)}

Dekripsi

- (p_1,p_2) = $(17,27) - 3(27,0) = (14-21)(16-9)^{-1}$ mod 31

  $= (17,27) - 6a = (17,27) - (27,0)$

  λ = $(0-27)(27-17)^{-1} mod\ 31$ = 19

  x_3 = λ^2-x_1-x_2 = 19^2-17-27 mod 31 = 7

  y_3 = λ (x_1-x_3)-y_1 = 19(17-7)-8 mod 31 = 8

  Maka hasil dari dekripsi ciphertext adalah {(7,8))}