Tugas Kriptografi

“Elliptic Curve”

Disusun Oleh:

Angga Kresnabayu (140810160001)

Prodi S1 Teknik Informatika

Fakultas Matematika dan Ilmu Pengetahuan Alam

Universitas Padjadjaran

2018

Soal

Diberikan persamaan elips, dengan nilai p = 29, a = 1, b = 6. Cari anggota yang menjadi Quadran Residu (QR) dan berapa saja pembangkitnya?

Jawab

a. Pembuktian

Rumus Persamaan Elliptic Curve:

- $y^2 \equiv x^3 + ax + b \pmod p$

Dengan Syarat:

- p>3 dan prima p=29 (Terpenuhi)
- $4a^3 + 27b^2 \neq 0$ $976 \neq 0$ (Terpenuhi)
- Maka persamaan $y^2 \equiv x^3 + x + 6$ merupakan persamaan Elliptic Curve

b. Mencari Quadran Residu

Rumus Quadran Residu

- $R^{(p-1)/2} \equiv 1 \pmod P$

R	$R^{(29-1)/2} \equiv 1 \pmod{29}$	$R \equiv 1$	Anggota QR(29)
0	$0^{14} \equiv 1 \pmod{29}$	0	NO
1	$1^{14} \equiv 1 \pmod{29}$	1	YES
2	$2^{14} \equiv 1 \pmod{29}$	28	NO
3	$3^{14} \equiv 1 \pmod{29}$	28	NO
4	$4^{14} \equiv 1 \pmod{29}$	1	YES
5	$5^{14} \equiv 1 \pmod{29}$	1	YES
6	$6^{14} \equiv 1 \pmod{29}$	1	YES
7	$7^{14} \equiv 1 \pmod{29}$	1	YES
8	$8^{14} \equiv 1 \pmod{29}$	28	NO
9	$9^{14} \equiv 1 \pmod{29}$	1	YES
10	$10^{14} \equiv 1 \pmod{29}$	28	NO
11	$11^{14} \equiv 1 \pmod{29}$	28	NO
12	$12^{14} \equiv 1 \pmod{29}$	28	NO
13	$13^{14} \equiv 1 \pmod{29}$	1	YES
14	$14^{14} \equiv 1 \pmod{29}$	28	NO
15	$15^{14} \equiv 1 \pmod{29}$	28	NO

16	$16^{14} \equiv 1 \pmod{29}$	1	YES
17	$17^{14} \equiv 1 \pmod{29}$	28	NO
18	$18^{14} \equiv 1 \pmod{29}$	28	NO
19	$19^{14} \equiv 1 \pmod{29}$	28	NO
20	$20^{14} \equiv 1 \pmod{29}$	1	YES
21	$21^{14} \equiv 1 \pmod{29}$	28	NO
22	$22^{14} \equiv 1 \pmod{29}$	1	YES
23	$23^{14} \equiv 1 \pmod{29}$	1	YES
24	$24^{14} \equiv 1 \pmod{29}$	1	YES
25	$25^{14} \equiv 1 \pmod{29}$	1	YES
26	$26^{14} \equiv 1 \pmod{29}$	28	NO
27	$27^{14} \equiv 1 \pmod{29}$	28	NO
28	$28^{14} \equiv 1 \pmod{29}$	1	YES

QR(29) = {1, 4, 5, 6, 7, 9, 13, 16, 20, 22, 23, 24, 25, 28}

c. Mencari Pembangkit

x	$x^3 + x + 6 \pmod{p}$	≡	In QR(29)	y
0	6 (mod 29)	6	YES	8,21
1	8 (mod 29)	8	NO	
2	16 (mod 29)	16	YES	4,25
3	36 (mod 29)	7	YES	6,23
4	74 (mod 29)	16	YES	4,25
5	136 (mod 29)	20	YES	7,22
6	228 (mod 29)	25	YES	5,24
7	356 (mod 29)	8	NO	
8	526 (mod 29)	4	YES	2,27
9	744 (mod 29)	19	NO	
10	1016 (mod 29)	1	YES	1,28
11	1348 (mod 29)	14	NO	
12	1746 (mod 29)	6	YES	8,21
13	2216 (mod 29)	12	NO	
14	2764 (mod 29)	9	YES	3,26
15	3396 (mod 29)	3	NO	
16	4118 (mod 29)	0	NO	
17	4936 (mod 29)	6	YES	8,21
18	5856 (mod 29)	27	NO	

19	6884 (mod 29)	11	NO	
20	8026 (mod 29)	22	YES	14,15
21	9288 (mod 29)	8	NO	
22	10676 (mod 29)	4	YES	2,27
23	12196 (mod 29)	16	YES	4,25
24	13854 (mod 29)	21	NO	
25	15656 (mod 29)	25	YES	5,24
26	17608 (mod 29)	5	YES	11,18
27	19716 (mod 29)	25	YES	5,24
28	21986 (mod 29)	4	YES	2,27

Pembangkit-pembangkitnya

x,y	x,y
0,8	0,21
2,4	2,25
3,6	3,23
4,4	4,25
5,7	5,22
6,5	6,24
8,2	8,27
10,1	10,28
12,8	12,21
14,3	14,26
17,8	17,21
20,14	20,15
22,2	22,27
23,4	23,25
25,5	25,24
26,11	26,18
27,5	27,24
28,2	28,27