ARGOS 동계 세미나_0204

201502086 이성복

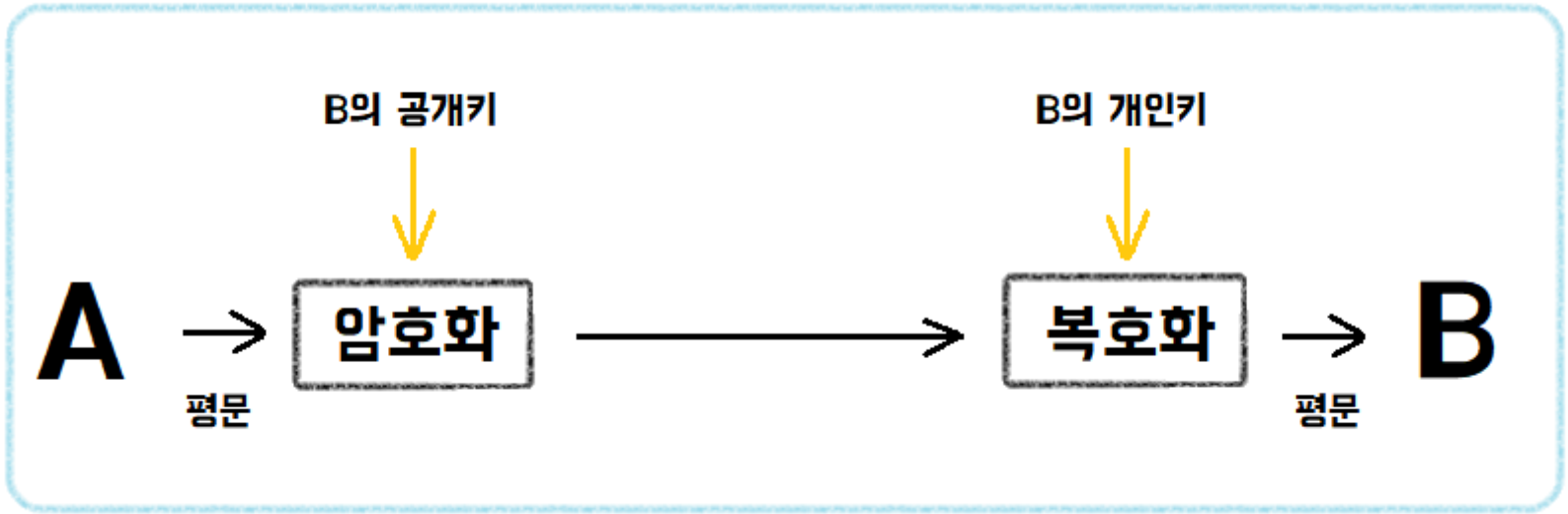
contents

- RSA
- Elliptic Curved Cryptography(ECC)

공개키 암호화

공개키 암호화

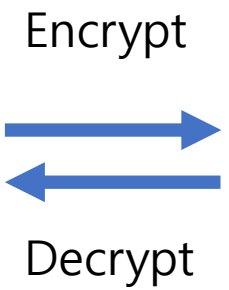
= 비대칭키 암호화



출처 : https://www.crocus.co.kr/1236

RSA

Easy algorithm

Prime number * Prime number 

Number

RSA

Easy algorithm

- Two prime number : 7, 13 → Max value is 91
- My public key : 5
- Use Extended Euclidean Algorithm → return 29

RSA

Easy algorithm

SEMINAR

A	B	C	D	E	F	G	H	I	J	K	L	M
65	66	67	68	69	70	71	72	73	74	75	76	77
N	O	P	Q	R	S	T	U	V	W	X	Y	Z
78	79	80	81	82	83	84	85	86	87	88	89	90

SEMINAR 83, 69, 77, 73, 78, 65, 82

출처 : https://blog.cloudflare.com/a-relatively-easy-to-understand-primer-on-elliptic-curve-cryptography/

RSA

Easy algorithm

SEMINAR 83, 69, 77, 73, 78, 65, 82

- 83 * 83 = 6889 is bigger than 91
- 6889 % 91 = 64

- 64 * 83 = 5312 % 91 = 34

- 5 times then result is 64

- 64 * 29 = 1856 is bigger than 91
- 1856 % 91 = 36

- 36 * 29 = 1044 % 91 = 43

- 29 times then result is 83

RSA

한계

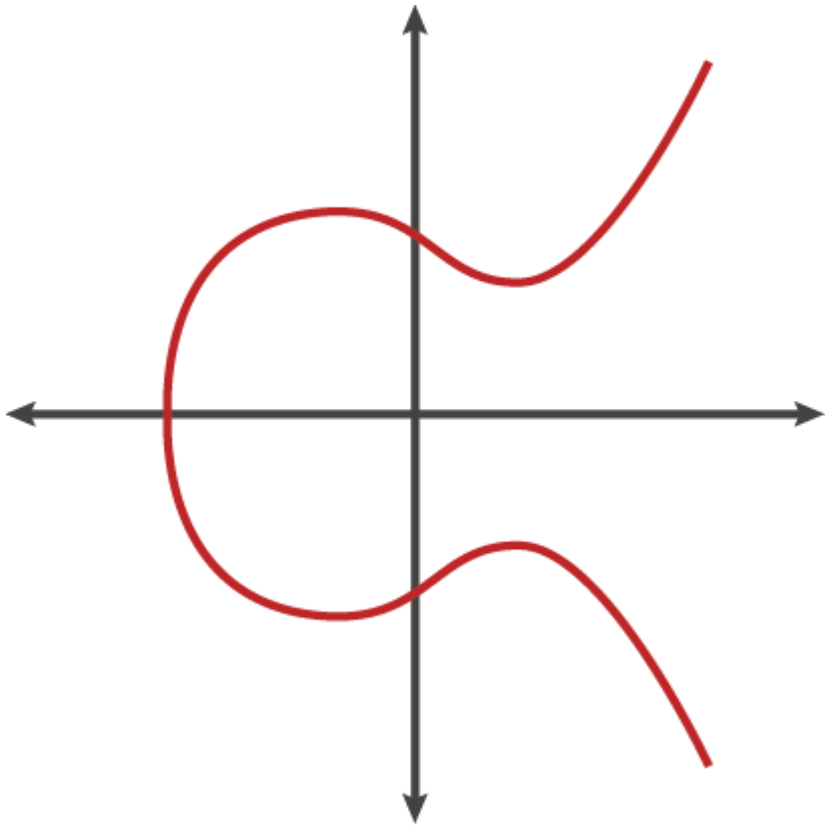
- Quadratic Sieve, General Number Field Sieve Algorithm
- This algorithm works well in large number

Elliptic Curved Cryptography

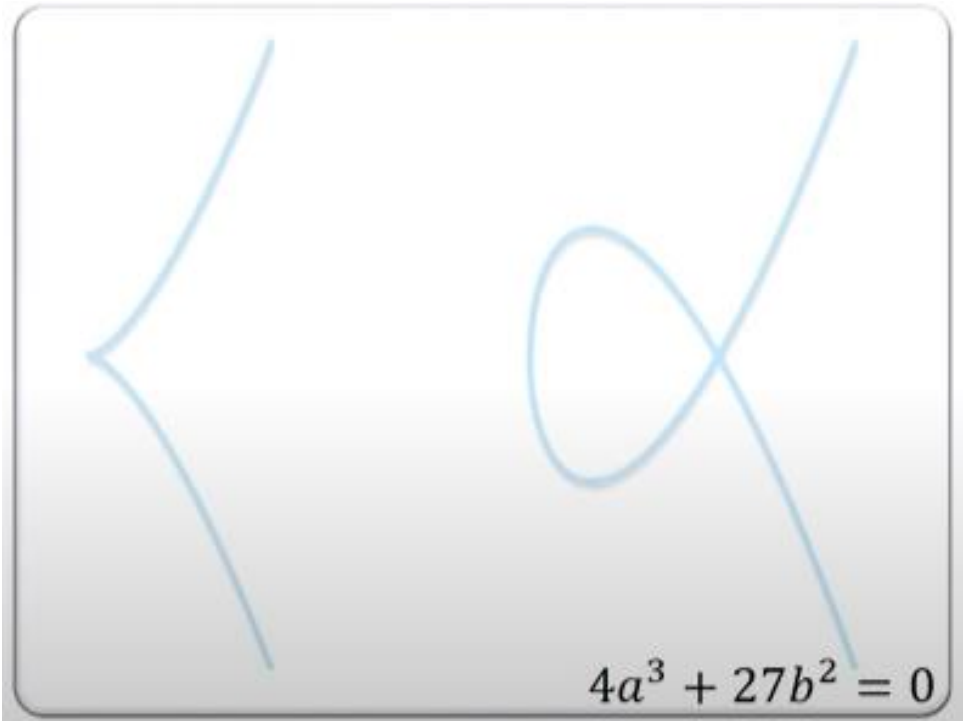
Elliptic Curved Cryptography

Elliptic Curve

$y^2 = x^3 + ax + b$ (Normal)



$4a^3 + 27b^2 = 0$ (Singularity)



출처 :
https://www.youtube.com/watch?v=_GOmrsCbNss

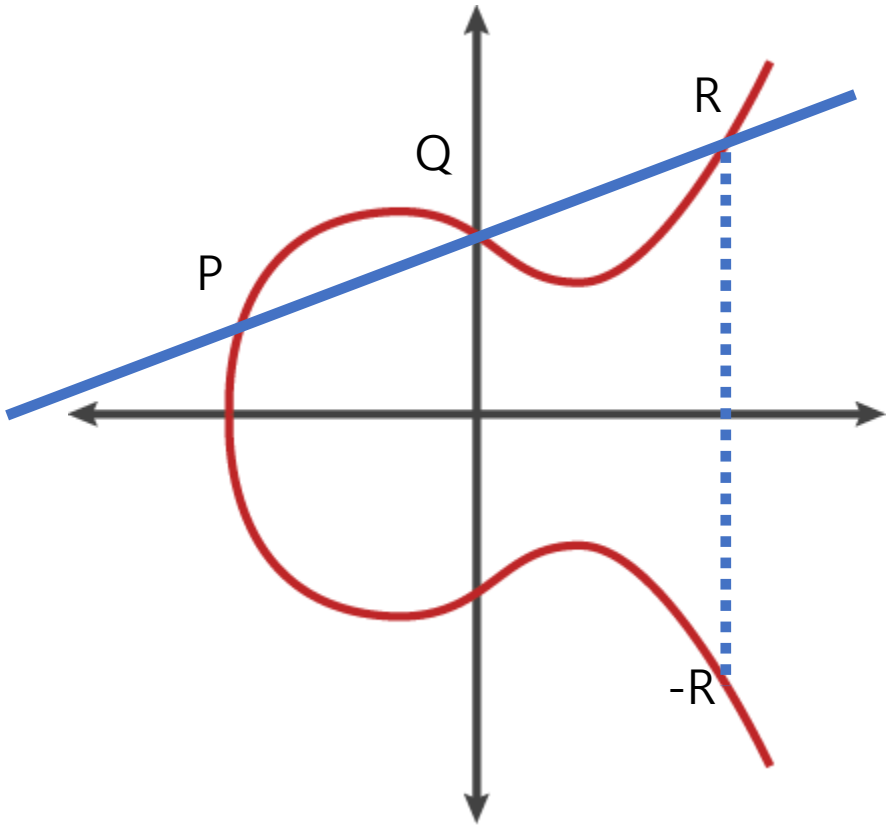
Elliptic Curved Cryptography

Real number field

We know P, Q

$y^2 = x^3 + ax + b$

$y = y_p + m(x - x_p)$



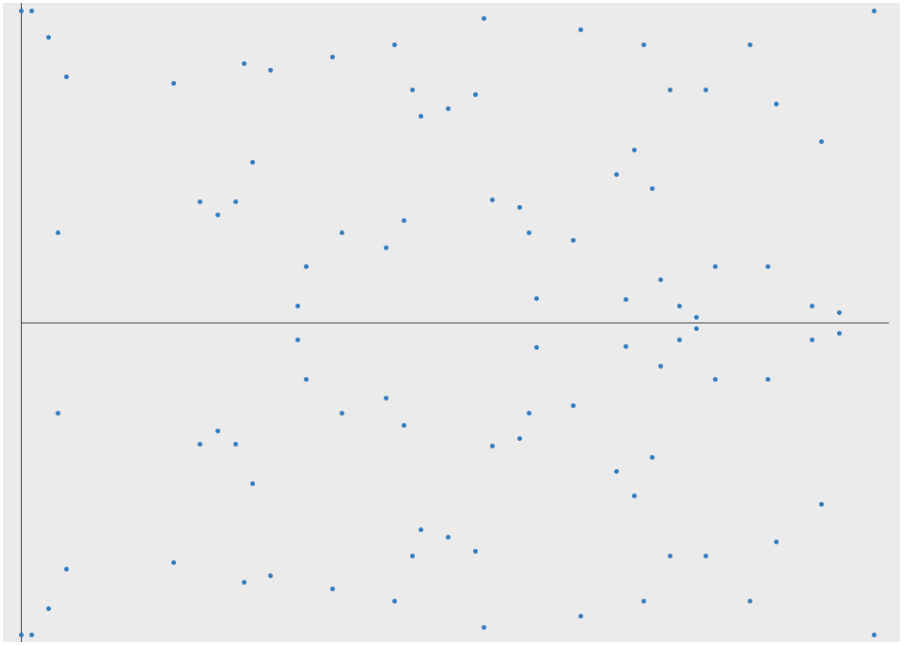
- Operation(+)
- Closed
- Associative
- Identity, Inverse element

Elliptic Curved Cryptography

Finite field F_p, Extended Euclidean

$y^2 = x^3 - x + 1 \pmod p$

$p = 97$



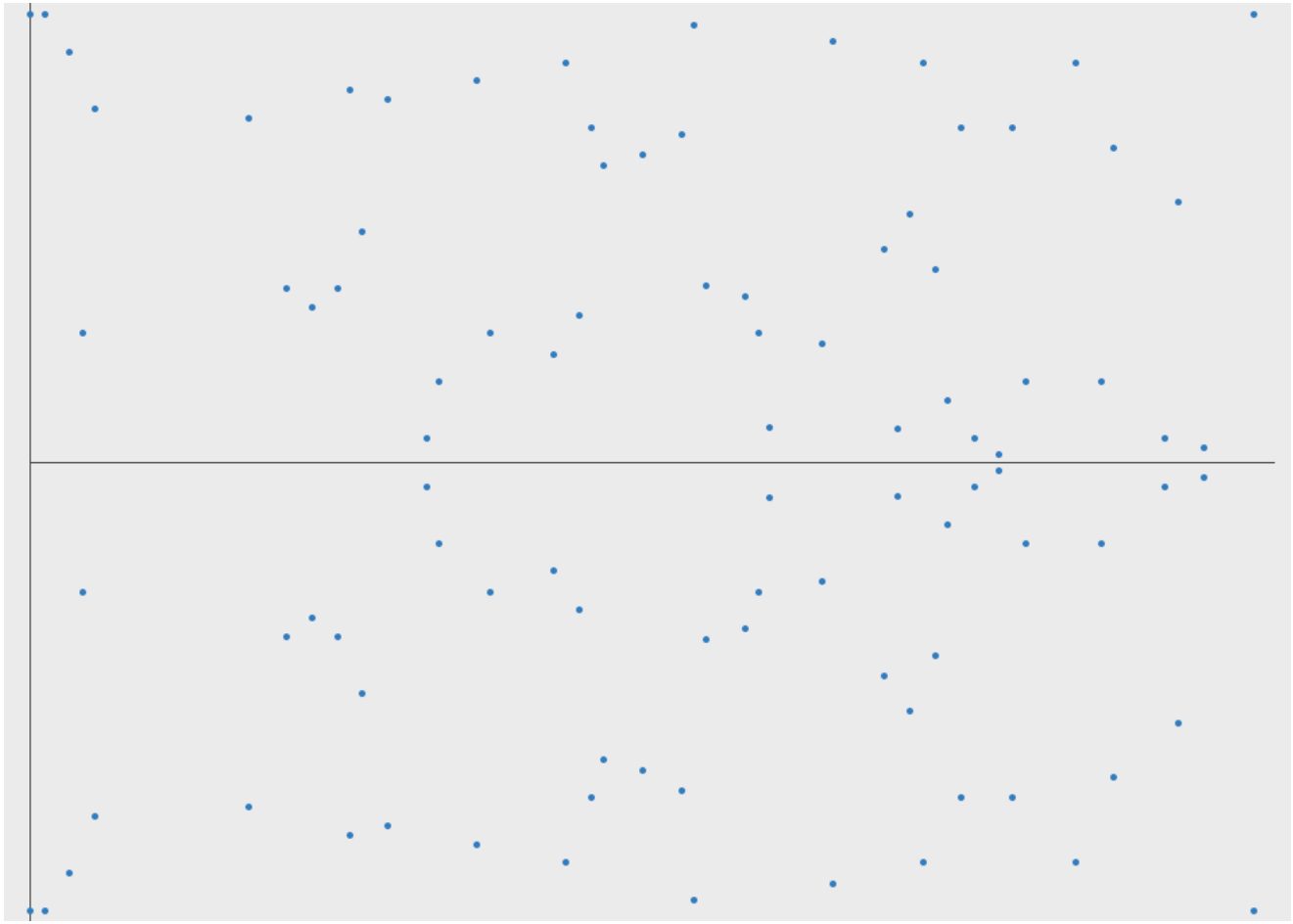
- Operation(+ , *)
- Closed
- Associative and Commutative, Distributive
- Identity, Inverse element
- p is prime number

출처 : https://blog.cloudflare.com/a-relatively-easy-to-understand-primer-on-elliptic-curve-cryptography/

Elliptic Curved Cryptography

Finite field, Extended Euclidean

$y^2 = x^3 - x + 1$
(mod 97)



출처 : https://blog.cloudflare.com/a-relatively-easy-to-understand-primer-on-elliptic-curve-cryptography/

Question