- ECC 암호화
- 타원곡선 이론에 기반한 공개 키 암호 방식이다.
- 타원곡선 상의 점 P에 정수 k를 곱하는 점 스칼라 곱셈 Q=kP로 정의되며 타원곡선 위에 존재하는 좌표 값들의 계산이기 때문에 암호화 연산에 필요한 비밀키 데이터는 모두 숫자거나 숫자로 변환이 필요하다.

- 공개키
- 공개키 암호 방식에서 사용하는 한 실체가 소유하는 키 쌍 중에서 공개되는 키

- 개인키
- 공개키 암호 알고리즘에서 사용되는 비대칭 키 쌍 중에서 공개되지 않고 비밀리에 사용하는 개인 키

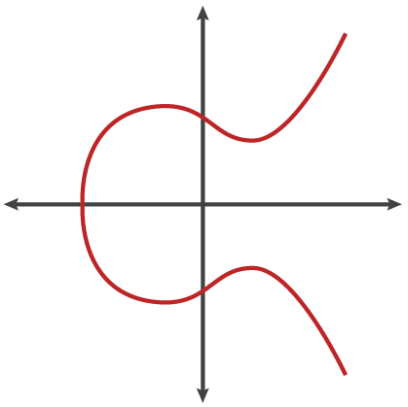
- 모듈러 연산
- 정수 나머지를 구하는 연산을 말한다.

- 유한체(GF)
- 유한개의 원소를 가지는 체를 말한다.

- 이산대수 문제
- 모듈러 연산으로 나머지만을 취하는 잉여계 시스템에서 위수를 구하는 것이 어렵다는 문제이다

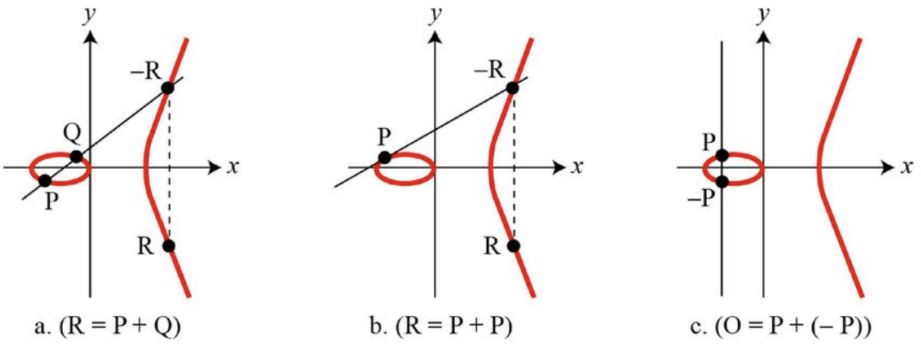
- 타원곡선
- 아래 방정식을 만족하는 x, y의 집합을 나타낸 곡선 그래프

$$y^2 = x^3 + ax + b, (4a^3 + 27b^2 \neq 0)$$



<타원곡선 그래프>

- 타원곡선 상에서의 연산(타원곡선 상의 덧셈 연산)
- 타원곡선 위 점 P와 점 Q를 지나는 직선이 타원과 만나는 교점 R을 x축으로 대칭시킨 점을 P+Q=R로 정의한다.



- Addition $(P \neq Q)$

$$\lambda = \frac{y_2 - y_1}{x_2 - x_1}$$
$$x_3 = \lambda^2 - x_1 - x_2$$
$$y_3 = (x_1 - x_3)\lambda - y_1$$

- Doubling $(P = Q)$

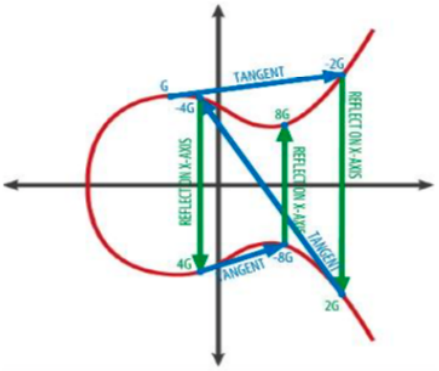
$$\lambda = \frac{3x_1^2 + a}{2y_1}$$
$$x_3 = \lambda^2 - 2x_1$$
$$y_3 = (x_1 - x_3)\lambda - y_1$$

- ECC 암호화 과정
- G : 생성자, 타원곡선 상의 임의의 점
- x : 개인키, P보다작은 소수로, 난수 생성기로 생성
- Q : 공개키, 개인키로부터 연산

점 P(x,y)가 타원곡선 상에 위치해 있을 때 두 점 P, Q와 임의의 정수 x에 대해 다음과 같은 방정식을 정의할 수 있다.

$$Q = xG$$

x의 값을 구하는 것은 타원곡선 이산대수 문제인데, 공개키 Q=xG=G+G+…+G로 G를 x번 더한 값이다.
이때 Q=xG 수식에서 x와 G를 구하기 쉽지만, 알려진 G값과 Q값을 통해 x값을 구하기 어려운 점을 이용하며 이것을
ECDLP(Elliptic Curve Discrete Logarithm Problem)라고 부른다. 이러한 속성으로 인해 공개키 암호 기술로 사용된다.



xG 연산 과정

출처

- dev_mac-_-. “기초암호학(4) - ECC(타원곡선 암호화 알고리즘). 티스토리, 2019.04.13.
- 최준백신경욱, 2021, 타원곡선 기반 공개키 암호 시스템 구현을 위한 Scalable ECC 프로세서, <한국정보통신학회논문지>
- 김현수박석천, 2011, 음성 데이터 보안을 위한 효율적인 ECC 암호 알고리즘 설계 및 구현, <한국정보통신학회논문지>