I.서론

1,연구의 필요성 또는 동기

현재 암호화 체계 **RSA** 암호화 알고리즘이 대표적으로 사용되고 있다. 하지만 **RSA** 알고리즘보다 **ECC** 알고리즘이 더 장점이 많다. 우리는 어떤 요소로 인하여 성능 차이가 나는지 궁금해져, 이를 분석하기로 했다.

2.연구문제

RSA 암호화가 어떤 요소로 인해 **ECC** 알고리즘에 비해 성능 차이가 날까**?**

II. 이론적 배경

3-1. RSA 공개키 방식: 현재 실생활에서 가장 많이 사용되고 있는 대표적인 양방향 데이터 암호화 기법이다.

***양방향 암호화: 암호화된 암호문을 복호화할 수 있는, 즉 사람이 알기 쉽게 처리할 수 있는 알고리즘을 의미한다.

RSA에 사용되는 연산방식은 모듈러 연산인데, 이는 어떤 한 숫자를 다른 숫자로 나눈 나머지를 구하는 연산을 의미한다.

***RSA** 알고리즘이 암호화되는 간략한 과정

1. 각각 **n, e, n, d**라는 두 정수로 이루어진 공개키와 개인 키를 만든다. 이때 **n**은 임의의 두 소수 **p.q**를 정하고 **n=p*q**를 해주면 **n**을 구할 수 있다.

2. e 구하기:**Φ(n) = (p - 1) * (q - 1)** 식을 이용하여 **Φ(n)**을 구한후, **e**는 **1 < e < Φ(n)**로써 **1**과 **Φ(n)** 사이에 있고 **Φ(n)**와 서로소인 **e**를 정해주면. 공개키에 이용되는 **e**를 구할 수 있다.

3. d 구하기: **(e * d) mod Φ(n) = 1** 즉, **e*d**를 **Φ(n)**으로 나누었을 때 나머지가 **1**인 **d**를 구한다.

3-2. ECC 암호화: 타원곡선 이론에 기반한 공개 키 암호 방식으로, 타원곡선 위의 임의의 점 **P**에 정수 **k**를 곱하는 점 스칼라 곱셈 **Q=kP**로 정의된다.

***공개키 암호화 방식:** 암호학적으로 연관된 두 개의 키를 만들어서 하나는 자신이 보관하고 다른 하나는 상대방에게 공개하는 것을 말한다. 다른 사용자와 키를 공유하지 않더라도 암호를 통한 통신을 할 수 있다는 장점이 있다.

타원곡선 위의 점들, 즉 좌푯값들의 계산이므로 비밀키 데이터는 모두 숫자여야 한다.

우선 타원곡선 위의 점들의 연산을 알아야 한다.

타원곡선 위의 점 **P**와 점 **Q**를 지나는 직선이 타원과 만나는 교점 **R**을 **x**축으로 대칭시킨 점을 **P+Q=R**로 정의한다.

***ECC** 암호화 과정

-G:생성자, 타원곡선 위의 임의의 점

-x:개인 키, **P**보다 작은 소수로, 난수 생성기로 생성

-Q:공개키, 개인 키로부터 연산

점 **P(x,y)**가 타원곡선 위에 위치할 때 두 점 **P, Q**는 임의의 정수 **x**에 대하여 **Q=xG**라는 방정식이 성립한다.