RSA, ECC 알고리즘 성능 분석 실험 계획서

알고리즘 성능에 영향을 미치는 요인 분석

1) 실험 목적

각 알고리즘의 어떤 요소가 성능(암호화 속도 및 용량 효율성)에 영향을 미치는 지 알기 위함이다.

2) 실험 과정

1. 각 알고리즘의 암호화 과정을 분석하고 세분화한다. 1)
2. 암호화 코드를 1 의 과정에서 세분화한 것에 따라 시간을 재는 코드를 삽입한다.
3. 각 코드를 10 만 번 반복 실행시켜 걸린 시간의 평균값을 얻는다. 2)
4. 위의 실험에서 얻은 결과를 바탕으로 알고리즘의 어떤 요소가 암호화의 성능에 어느 정도의 영향을 미치고 있는지 확인한다.

1) 이 실험에서는 키 생성을 위한 소수 준비, 공개키와 비밀키 생성, 암호화 총 3 개 과정으로 구분했다.

2) 반복 실행 횟수를 10 만 번으로 정한 근거는 횟수를 5 만 번부터 10 만 번까지 점차 올렸을 때 결괏값의 변동이 거의 없었기 때문이다. 따라서 그 이상의 반복 수행은 무의미할 것으로 보고 10 만 번으로 결정하였다.

RSA, ECC 알고리즘 성능 분석 실험 보고서

1) 실험 데이터

https://github.com/Trifa0527/2023math 참고

1. RSA 데이터 분석

RSA 알고리즘은 키 생성을 위한 소수 준비 과정에서 0.000196 초를, 공개, 비밀키 생성 과정에서 0.220435 초, 암호화 과정에서 0.000012 초로 총 0.220644 초가 소요되었다.

2. ECC 데이터 분석

2) 결론

두 알고리즘 모두 총 암호화 시간 중에서 공개, 비밀키 생성 과정이 가장 큰 비율을 차지하였다. 이 과정에 비하면 나머지 소수 준비 과정과 암호화 과정은 무시할 수 있을 정도이다. 따라서 알고리즘의 성능을 향상시키려 한다면 공개, 비밀키 생성 시간을 단축하는 것이 필수적이다.