

RSA, ECC 알고리즘 성능 분석 실험 계획서

알고리즘 간 성능 분석법

1) 실험 목적

두 알고리즘의 암호화 속도를 비교하여 성능의 차이를 확인하기 위함. 이때 성능의 차이라고 함은 단순 암호화 속도로 간주한다.

알고리즘을 개선하여 성능을 비교할 때도 같은 방식으로 진행한다.

속도가 빠를수록 성능이 높다.

2) 실험 과정

1. RSA, ECC 알고리즘을 구현한다.
2. 동일한 비교를 위하여 같은 문자열을 준비한다.(4 자리 문자열, 12 자리 문자열 각 10 만개씩)
3. 실험환경을 구성한다. 저성능의 경우 아마존 클라우드 서비스에서 제공하는 무료 서버를 (AWS EC2 t2.micro RAM 1G) 고성능의 경우 개인용 컴퓨터 (애플 M1 8 코어 RAM 8G)를 활용한다.
4. 알고리즘 별로 각 환경에서 2 번에서 준비한 문자열을 5 번씩 암호화한다. 이때 걸린 시간을 측정한다.