**20160521 이준희 CS443 Lab3 Report**

**코드 설명**

Part1

Cryptograph에 대한 부분으로 msg 해쉬 값을 SHA512로 구하고 RSA를 통해 암호화한다. Sign(sk, msg) 함수로 나온 sig는 verify(pk, sig, msg)를 통해 확인할 수 있다.

Part2

DBManager를 통해 블록과 블록 안의 트랜잭션, 블록 간의 연결을 관리 할 수 있다. 이후 verifty/validate에서 각각의 블록과 트랜잭션이 제대로 된 값을 가지고 있는 지 확인하고 Part1을 통해 해쉬 값과 사인 값으로 유효성을 확인할 수 있다. 마지막으로 miner에서 직접 nonce를 1씩 증가시키면서 PoW 작업으로 mining한다.