**과제2: 30-bit triple RSA 구현**

* 수업시간에 배운 RSA 암호화를 바탕으로 직접 RSA 암호화, 복호화를 수행하는 프로그램을 구현한다.

**제출** **기한**

* 12월 8일 오후 11:59

**구현조건**

1. 구현 언어: C, C++로 구현
2. 키 생성(Key Generation)에서 이고 의 각각 크기는 15bit이다.
   1. p, q의 범위는 2^14 이상 2^15 - 1 이하이다. (15bit에서 MSB가 1)
3. 는 rand, srand 와 같은 일반 random number generator를 이용한다.
4. 구현 시 포함해야 하는 알고리즘은 다음과 같다.
   1. Square and multiply algorithm for modular exponentiation
   2. Miller-Rabin Primality test (테스트는 20회로 설정)
   3. Extended Euclidean Algorithm
   4. Chinese Remainder Theorem
5. 사용자로부터 정수 형태의 메시지를 받아 메시지를 암호화·복호화 한 결과를 보인다.

**제출물**

1. 보고서 (pdf 파일로 제출)
2. 압축파일
   1. 보고서 원본 파일(docx, hwp 등)
   2. exe 실행 파일
   3. 소스코드 파일

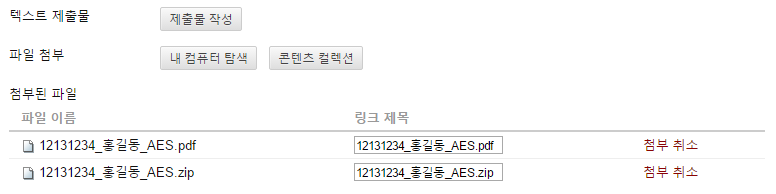
(비주얼 스튜디오 프로젝트 형태로 제출해도 됩니다. MAC에서 작업한 코드는 채점이 불가합니다.)

**과제** **채점** **기준**

* RSA 암호화 복호화 구현 (70점)
  + Square and multiply algorithm for modular exponentiation 구현 (10점)
  + Miller-Rabin Primarlity test 구현 (15점)
  + Extended Euclidean Algorithm 구현 (15점)
  + 암호화 과정 (10점)
  + 복호화 과정 – 반드시 Chinese Remainder Theorem으로 구현할 것 (20점)
* 보고서 (20점)
  + 구현 환경 및 구현 언어 기재 (MAC 사용 불가)
  + AES 암호화, 복호화 각 단계 설명 및 코드 설명 기재
* 코드 주석 및 제출 방법 숙지 (10점)

**제출방법**

* pdf파일과 압축 파일을 각각 올릴 것. 제출 방법 위반 시 감점 있음.
* 보고서와 압축파일 이름을 ‘<학번>\_<이름>\_RSA.\*’로 지정. (예. 12131234\_홍길동\_RSA.pdf)



**RSA 결과 출력 예제**

