과제 #2
미니 RSA 구현
2016-11-15

목표

알고리즘 내부에서 다루게 될 파라미터들의 길이가 32bit를 넘지 않는 간단한 RSA를 구현해 본다.
이렇게 구현된 RSA는 키의 길이가 너무 짧아 비실용적이지만, 알고리즘의 동작 원리를 이해하기에는 충분하다.

구현요약

사용되는 숫자 값의 크기가 최대 2^{32}를 넘지 않는 mini RSA를 구현한다.
과제는 c언어로 작성하도록 하며, 제한사항에 주어진 조건들을 만족하도록 구현한다.
코드 수행 중 값들이 정상적으로 연산되는지 확인하기 위한 중간 처리과정을 보여준다.

제한사항

- 구동 및 테스트 환경은 Linux 환경에서 gcc를 사용하여 컴파일 하는 것을 기본으로 하며, Windows 에서는 Cygwin을 설치하여 컴파일을 수행하도록 한다.(MS Visual Studio 이용해 작성하지 않도록 한다.)
- 파라미터들의 기본 자료형으로써 4byte 'unsigned int'를 'uint'로 정의하여 사용하도록 하며, 이 보다 더 큰 (4byte 이상의) 자료형은 사용하지 않도록 한다.
- 주어진 뼈대코드에서 임의 수 생성을 위한 RNG(Random Number Generator)는 rsa.h 파일에 구현된 $0 \leq r < 1$ 사이의 값을 duoble 형으로 반환해주는 'WELLRNG512a' 함수를 사용하도록 한다.
- 전체 알고리즘에서 사용되는 나눗셈, 나머지(모듈러) 연산을 c언어에서 지원하는 연산자('/', '%')를 사용하지 않고 비트 연산으로 처리하도록 한다.
- 거듭제곱 연산을 할 때 'square and multiply' 알고리즘을 이용하여 빠르게 연산되도록 한다.
- 모듈러 값 n이 $2^{31} \leq n < 2^{32}$(32bit 수)가 되도록 두 소수 p, q를 임의로 선택한다.
- p, q는 Miller-Rabin 소수 판별법과 같은 확률적인 방법을 사용하여, 이론적으로 4N(99.99%) 이상 되는 값을 선택하도록 한다.
- 조건을 만족하는 적절한 e값을 임의로 선택하여 사용하고, e의 $\mathrm{mod}\ \Phi(n)$에서 역수 d를 찾는 방법은 확장 유클리드 알고리즘을 사용하도록 한다.
- 키 생성에 성공하면 (e, n)이 공개키가 되고 (d, n)이 개인키가 되도록 하여 암•복호화에 사용한다.
- 암•복호화에 사용되는 메시지 M은 byte stream 형태로 간주한다. (단순히 cmd 창에서의 ASCII 코드 입력만을 고려하여 구현하지 않는다.)
- 암•복호화에 사용되는 데이터 블록의 기본 단위는 32bit(4byte)이다.
- 블록 단위로 조각낸 데이터를 암•복호화 할 때 공간이 비면, 남는 bit는 0으로 패딩 후 처리하여 고정된 크기로 연산될 수 있도록 한다.
- 블록 단위로 조각난 데이터의 값이 모듈러 n값 보다 큰 경우엔 암•복호화 할 수 없으므로 오류로 처리한다.

참고사항

- 타인의 코드를 전체 혹은 일부 사용하여 작성하는 경우에는 이유 불문하고 상호 F학점으로 처리한다.
- mini RSA에 관한 이론적인 기준은 수업 PPT를 중심으로 위의 제한사항을 참고하도록 한다.
- 모듈러 곱 연산 간 발생할 수 있는 오버플로우에 대한 처리가 되어 있어야 한다.
- 기작성된 main 함수는 주어진 파일 입력을 읽어 암호화를 진행하고, 암호화된 파일을 다시 읽어 복호화 한 뒤 다른 파일에 저장하도록 작성 되었으나, 구현의 방향이나 결과물의 출력에 따라 수정하여 사용하여도 된다.
- 다른 함수들 또한 입출력 파라미터를 지정해두었으나, 구현과정에서 추가 혹은 삭제, 수정하여 사용 가능하다.
- 암•복호화 결과물과 중간 연산과정은 화면 출력 혹은 파일로 저장하도록 하며, 블록 단위로 나누어 진 데이터와 암호화 된 값, 복호화 된 값 등을 기록하여 RSA가 잘 진행되고 있는지 보여줄 수 있도록 한다.
- 개인키와 공개키를 위한 e, d, n 값과 이를 검산하기 위한 값 또한 출력 결과물에 포함되어 있어야 한다.
- 모든 입력과 출력에 대한 예외처리가 되어 있어야 한다.

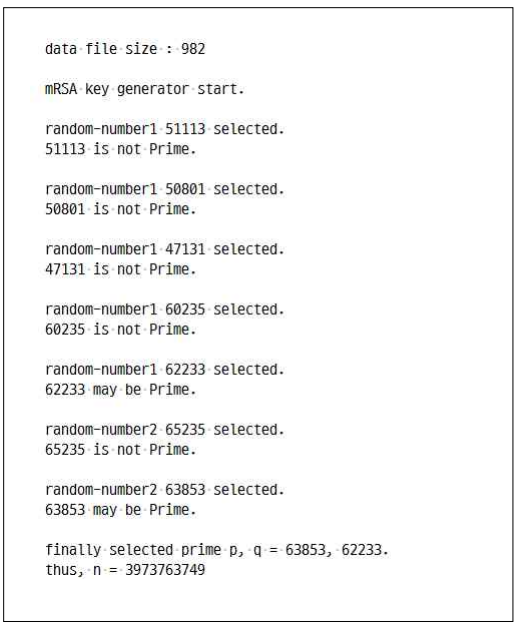
제출물 (임시)

미니 RSA 소스코드와 테스트 실행 결과가 담긴 파일을 마감기한 전까지 “학번_이름_miniRSA.zip”의 형태로 압축한 뒤 “암호학_과제_#2_학번_이름”의 제목으로 [siera@hanyang.ac.kr]에 제출한다.

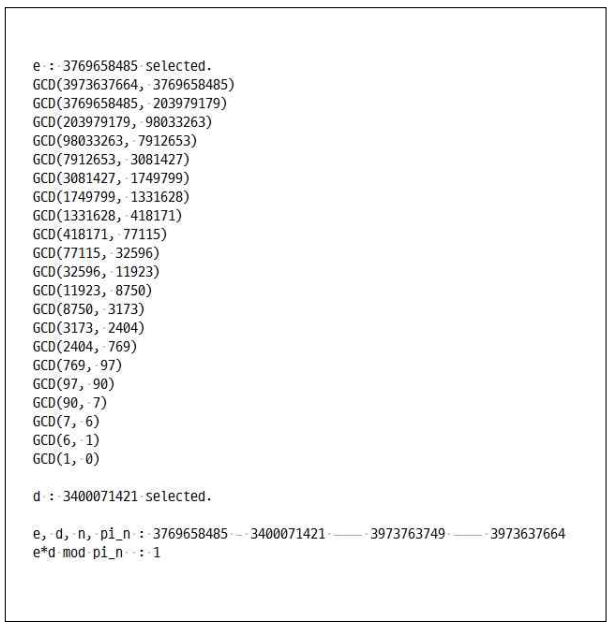
마감기한 (임시)

- 마감일 : 2016년 12월 03일 토요일 자정 전까지
- 페널티 : 마감일을 넘겨 제출할 경우, 해당 과제의 최고점부터 채점을 시작하여 하루 단위로 20%씩 감점된다. 예를 들어 마감기한에서 하루가 지난 다음날 제출하였을 경우에 최고점이 20점, 본인 취득점수가 18점 이라면, 18점의 80%인 14.4에서 반올림 한 14점을 받게 된다.

코드 수행 예시



```
data file size : 982

mRSA key generator start.

random-number1 51113 selected.
51113 is not Prime.

random-number1 50801 selected.
50801 is not Prime.

random-number1 47131 selected.
47131 is not Prime.

random-number1 60235 selected.
60235 is not Prime.

random-number1 62233 selected.
62233 may be Prime.

random-number2 65235 selected.
65235 is not Prime.

random-number2 63853 selected.
63853 may be Prime.

finally selected prime p, q = 63853, 62233.
thus, n = 3973763749
```



```
e : 3769658485 selected.
GCD(3973637664, 3769658485)
GCD(3769658485, 203979179)
GCD(203979179, 98033263)
GCD(98033263, 7912653)
GCD(7912653, 3081427)
GCD(3081427, 1749799)
GCD(1749799, 1331628)
GCD(1331628, 418171)
GCD(418171, 77115)
GCD(77115, 32596)
GCD(32596, 11923)
GCD(11923, 8750)
GCD(8750, 3173)
GCD(3173, 2404)
GCD(2404, 769)
GCD(769, 97)
GCD(97, 90)
GCD(90, 7)
GCD(7, 6)
GCD(6, 1)
GCD(1, 0)

d : 3400071421 selected.

e, d, n, pi_n : 3769658485 3400071421 3973763749 3973637664
e*d mod pi_n : 1
```

```
MRSACipher start. file len is 982.

len : 982
buf : plaiý
ptx : 1767992432
ctx : 3121955281

len : 978
buf : ntexý
ptx : 2019914862
ctx : 1120659761

len : 974
buf : t foý
ptx : 1868963956
ctx : 3026741705

len : 970
buf : r miý
ptx : 1768759410
ctx : 2270967476

len : 966
buf : ni Rý
ptx : 1377855854
ctx : 1443831680

len : 962
buf : SA eý
ptx : 1696612691
ctx : 3797745550
```

```
MRSACipher start. file len is 984.

len : 984
buf : ÑA<NAK>ª
ptx : 3121955281
ctx : 1767992432

len : 980
buf : 1éËB
ptx : 1120659761
ctx : 2019914862

len : 976
buf : Éih´
ptx : 3026741705
ctx : 1868963956

len : 972
buf : ´6\╤
ptx : 2270967476
ctx : 1768759410

len : 968
buf : €<USS>V
ptx : 1443831680
ctx : 1377855854

len : 964
buf : Žÿ\â
ptx : 3797745550
ctx : 1696612691
```