**Cryptography Program #3**

소프트웨어학부

2018044720 석예림

1. mod.c 소스코드

Text

Description automatically generated

Text

Description automatically generated

2. 코드 내 함수 설명

* uint64\_t mod\_add(uint64\_t a, uint64\_t b, uint64\_t m) : a + b mod m 계산하는 함수. a+b mod m = ((a % m) + (b % m)) % m으로 계산해도 가능하다. a+b<b일때 오버플로가 발생하기 때문에 b대신 b-m을 넣어 계산해준다.
* uint64\_t mod\_sub(uint64\_t a, uint64\_t b, uint64\_t m) : a – b mod m 계산하는 함수. a-b mod m = ((a % m) - (b % m)) % m 으로 가능하다.

a < b일때 결과가 음수가 되므로 (a % m) - (b % m) 빼기 해준 상태에서 m을 더해 양수로 만들어준 후 mod m해 준다.

* uint64\_t mod\_mul(uint64\_t a, uint64\_t b, uint64\_t m) : a \* b mod m 계산하는 함수. 오버플로 발생을 막기 위해 덧셈을 사용하여 계산하는 Double addition 알고리즘을 사용한다. Double addition 알고리즘은 b가 0이상이고 b의 해당 비트가 1이면 나머지 r에다가 r+a mod m 해주고 b비트를 하나 옮기고 a에 a를 더해 mod m해주며 b의 값이 0보다 작아질 때까지 계산해 준다.
* uint64\_t mod\_pow(uint64\_t a, uint64\_t b, uint64\_t m) : a ^ b mod m 계산하는 함수. Square multiplication 알고리즘을 사용한다. a^b mod m = (a mod m \* a mod m \* ... \* a mod m) mod m 로 계산되기 때문에 mod\_mul함수를 사용하여 a의 지수제곱한 결과에 mod m해준 값을 b의 비트가 1일때 나머지와 a를 곱해 계산한다.

3. 실행 결과

Text

Description automatically generated