

Cryptography Program #1

소프트웨어학부

2018044720 석예림

1) 코드 내 함수 설명

- `gcd()` : 유클리드 알고리즘인 $\text{gcd}(a, b) = \text{gcd}(b, a \bmod b)$ 을 사용하여 최대공약수를 구하도록 구현하였습니다.
- `xgcd()` : 확장형 유클리드 알고리즘인 $\text{gcd}(a, b) = d = ax + by$ 를 사용하여 $d_0 = a, d_1 = b, x_0 = 1, x_1 = 0, y_0 = 0, y_1 = 1$ 을 초기값으로 잡고 $q_i = d_{i-1} \div d_i, d_{i+1} = d_{i-1} - q_i d_i, x_{i+1} = x_{i-1} - q_i x_i, y_{i+1} = y_{i-1} - q_i y_i$ 의 식을 이용하여 $d_{k+1} = 0$ 일때, $*x = x_k$ 인 x_0 을 갖게 하고, $*y = y_k$ 인 y_0 을 갖게하고, d_0 를 return 시킵니다.
- `mul_inv()` : `xgcd()`를 변형하여 $d_1 == 1$ 일때, a 와 m 이 서로소이기 때문에 a 의 $\bmod m$ 에 대한 inverse를 구하게 됩니다.

1) 컴파일 과정과 실행 결과

```
yerim ~/Downloads/2020 암호학/프로그램 #1
> gcc 석예림_2018044720_euclid_skeleton.c
yerim ~/Downloads/2020 암호학/프로그램 #1
> ./a.out
gcd(28,0) = 28
gcd(0,32) = 32
gcd(41370,22386) = 42
gcd(22386,41371) = 1
---
42 = 41370 * -204 + 22386 * 377
41370^-1 mod 22386 = 0, 22386^-1 mod 41370 = 0
---
1 = 41371 * 4285 + 22386 * -7919
41371^-1 mod 22386 = 4285, 22386^-1 mod 41371 = 33452
Random testing.....No error found
yerim ~/Downloads/2020 암호학/프로그램 #1
>
```