Cryptography Program #1

소프트웨어학부
2018044720 석예림

1) 코드 내 함수 설명

- gcd() : 유클리드 알고리즘인 gcd(a, b) = gcd(b, a mod b)을 사용하여 최대공약수를 구하도록 구현하였습니다.

- xgcd() : 확장형 유클리드 알고리즘인 gcd(a, b) = d = ax + by 를 사용하여 d0 = a, d1 = b, x0 = 1, x1 = 0, y0 = 0, y1 = 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, d0 를 return 시킵니다.

- mul_inv() : xgcd()를 변형하여 d1==1 일때, a 와 m 이 서로소이기 때문에 a 의 mod m 에 대한 inverse 를 구하게 됩니다.

1) 컴파일 과정과 실행 결과