현대암호학기초

조별과제

9조 송희원, 권혜민, 이현정, 윤명지

**RSA의 키 쌍의 생성**

단, 주어진 소수 p = 41, p = 61로 지정

1. N = p x q = 41 x 61 = 2501
2. L= lcm(p-1, q-1) = lcm(40,60) = 120
3. 1 < e < L , gcd(e , L) = 1 -> e = 11
4. 1 < d < L , e x d mod L = 1 -> d = 11

**암복호화**

(평문 = 4로 설정)

**<암호화 과정>**

평문^e mod N

= 4^11 mod 2501

= 127

**4의 암호문 = 127**

**<복호화 과정>**

암호문^d mod N

= 127^11 mod 2501

= 4

**127의 평문 = 4**