1971027_오지은

소스 설명

1. 함수 구성

1. get_prime()
    a. 1 ~ pow(2, 16) 범위의 소수 리스트 리턴
2. gcd(a, b)
    a. a, b 서로수 여부 판별
3. get_e(phi)
    a. 2 ~ phi 사이면서 phi와 서로수인 e를 구함.
4. get_d(e, phi)
    a. e*d를 phi로 나누었을 때 나머지가 1인 d를 구함.

2. 복호화 플로우

1. get_prime()을 통해 소수 리스트를 구하고 그 안에서 p, q를 랜덤으로 선정
2. p, q를 이용해 n, phi를 구함.
3. get_e(), get_d()를 이용해 공개키 e와 개인키 d를 구함.
4. 메시지 M은 12345라고 가정.
5. 메시지 암호화 공식에 따라 암호화된 C를 구함.
6. 메시지 복호화 공식에 따라 복호화된 원 메시지 guessM을 구함.

실행결과

```
python -u "/Users/jieun/Desktop/4-2/네트워크보안/과제2 - RSA/source.py"
/과제2 - RSA/source.py"
p =  25189
q =  773
N =  19471097
phi =  19445136
e =  1195219
d =  787099
Message Input :  12345
**Encryption - cipher =  11897514
**Decryption - decrypted cipher =  12345
jieun@ojieun-ui-MacBookPro 과제2 - RSA %
```