**REPORT**

(프로그래밍 과제 4)

로고, 상징, 등록 상표, 폰트이(가) 표시된 사진

AI가 생성한 콘텐츠는 부정확할 수 있습니다.

|  |  |
| --- | --- |
| 이름 | 김민서 |
| 학과 | 컴퓨터인공지능공학부 |
| 학번 | 202213083 |
| 과목명 | 이산수학 |
| 교수님 | 신상욱 교수님 |
| 분반 | 101분반 |
| 제출일 | 2025.05.16 |

* **작은 정수에 대한 RSA 알고리즘 구현**
  + **컴퓨터의 기본적인 정수 연산을 이용한 간단한 RSA 암호 구현.**
  + **강의 자료 "Ch04\_Number-Theory-and-Cryptography-p2.pdf"**

**의 p.30~p.32 참고**

**Ex)**

**[키 생성]: 작은 크기의 두 개 소수 p와 q를 랜덤하게 선택하여 공개키와 개인키를 생성한다(100 이하의 소수를 생성해도 무방함).**

* **사용하는 프로그래밍 언어에서 지원하는 난수 생성 함수를 사용하여, p를 랜덤하게 선택한 후, 소수 검사 함수를 사용하여 소수인지 판정. 만약 소수가 아니면 다시 랜덤한 수 생성 후 소수 판정함. (강의 자료 "Ch04\_Number-Theory-and-Cryptography-p2.pdf"의 p.4 소수 검사 알고리즘 pseudo code 참고)**
* **q에 대해서도 돟일하게 동작**
* **z = p\*q**
* **phi = (p-1)\*(q-1)**
* **gcd(n, phi)=1 이 되는 n 선택 (간단한 예제의 경우, n은 3, 11, 23 등과 같은 소수를 선택해서 사용해도 된다).**
* **(n\*s) mod phi = 1 이 되는 s를 계산한다 (확장된 유클리드 알고리즘 사용).**
  + **(강의 자료 "Ch04\_Number-Theory-and-Cryptography-p2.pdf"의 p.21 'Extended Euclid Algorithm' pseudo code 참고)**

**==> 공개키와 개인키를 반환한다.**

**공개키 : (z, n)**

**개인키: s (p, q를 함께 비밀로 유지해도 된다)**

**[암호화]**

**평문 메시지로 정수 a (<z), 공개키 (z, n)을 입력 받는다.**

**다음과 같이 계산된 암호문 c를 반환한다.**

**c = a^n mod z**

**(강의 자료 "Ch04\_Number-Theory-and-Cryptography-p1.pdf"의 p.30 'Exponentiation Mod z by Repeated Squaring' pseudo code 참고)**

**[복호화]**

**암호문 c와 z, 그리고 개인키 s와를 입력받는다.**

**다음과 같이 계산된 평문 메시지 a를 반환한다.**

**a = c^s mod z**

**# 코드**

import random

import math

# 랜덤한 소수 생성 함수

def is\_PrimeNum(x):

    if (x < 2):

        return False

    for i in range(2, int(math.sqrt(x)) + 1):

        # 소수가 아닌 경우 False 반환

        if (x % i == 0):

            return False

    # 소수인 경우 True 반환

    return True

# 확장된 유클리드 알고리즘 함수

def extended\_gcd(a, b):

    if (a < b):

        a, b = b, a

    # 예외) b가 0인 경우

    if (b == 0):

        return a, 1, 0

    r = a % b

    gcd, x1, y1 = extended\_gcd(b, r)

    x = y1

    y = x1 - (a // b) \* y1

    return gcd, x, y

# 제곱 함수

def repeated\_squaring(a, n, z):

    result = 1

    base = a % z

    while (n > 0):

        if (n % 2 == 1):

            result = (result \* base) % z

        base = (base \* base) % z

        n //= 2

    return result

# 랜덤 p 생성

while (True):

    p = random.randint(1, 100)

    if is\_PrimeNum(p):

        break

# 랜덤 q 생성

while (True):

    q = random.randint(1, 100)

    if is\_PrimeNum(q):

        break

# z, phi, n, s값 생성

z = p \* q

phi = (p - 1) \* (q - 1)

n = 65537 #가장 대중적인 값

gcd, x, y = extended\_gcd(n, phi)

s = x % phi

print("해당 프로그래밍 리포트에서는 결과값 확인을 위해 모든 변수의 값을 출력해둔다.")

print("")

print("p : %d" %p)

print("q : %d" %q)

print("공개키(z, n) : (%d, %d)" %(z, n))

print("개인키(s) : %d" %s)

print("")

Enc\_A, Enc\_Z, Enc\_N = map(int, input("평문 메시지로 정수 a, 공개키 (z, n)을 입력하시오 : ").split())

print("암호문 메시지 :", repeated\_squaring(Enc\_A, Enc\_N, Enc\_Z))

print("")

Dec\_C, Dec\_Z, Dec\_S = map(int, input("암호문 c와 z, 그리고 개인키 s를 입력 하시오. : ").split())

print("평문 메시지 :", repeated\_squaring(Dec\_C, Dec\_S, Dec\_Z))

**# 실행 결과  
텍스트, 스크린샷, 폰트, 소프트웨어이(가) 표시된 사진

AI가 생성한 콘텐츠는 부정확할 수 있습니다.**

**평문 메시지 1357 + 공개키 -> 암호화 메시지 2416**

**암호화 메시지 2416 + 공개키 + 개인키 -> 평문 메시지 1357**