


MSSV: 19127102

Họ tên: Võ Hoàng Gia Bảo

* Hướng dẫn sử dụng code *

1. Mở file 19127102.py bằng PyCharm
2. Chạy file bằng cách nhấn tổ hợp Shift + F10 hoặc nhấn biểu tượng 
3. Nhập 2 số để tính ước chung lớn nhất bằng thuật toán bezout (Euclid mở rộng)
4. Sau khi đã tính ước chung lớn nhất, hệ thống sẽ random 2 số nguyên tố lớn

```
temp = random.randint(0, 10 ** 10)      # Could be 10 ** 128 -> 1024 bits
```

Có thể tùy chỉnh đến 128 chữ số (1024 bit). Mặc định random 10 chữ số

Sau khi random hệ thống sẽ kiểm tra có phải số nguyên tố “lớn” hay không bằng thuật toán rabin-miller

Source:

https://rosettacode.org/wiki/Miller%E2%80%93Rabin_primality_test#Python

5. Hệ thống sẽ output ra 2 cặp key là public key (e, n) và private key (d, n)

```
C:\Users\USER\AppData\Local\Programs\Python\
Input 2 numbers: 30 80
GCD of 80 and 30 is 10
ax + by = gcd(a, b) => 80*-1 + 30*3 = 10

Public key (e, n):
    e = 72452127871295297
    n = 109654457048039093

Private key (d, n):
    d = 45654760779823925
    n = 109654457048039093

Process finished with exit code 0
```

* Bài tập vành *



BT vành C/mình

1. $0x = x0 = 0 \quad \forall x \in \mathbb{Z}_n$

$x \cdot 0 = x(0+0) = x0 + x0$

$\Rightarrow x0 = 0$

Tương tự: $0x = (0+0)x = 0x + 0x \Rightarrow 0x = 0$

$\Rightarrow x0 = 0x = 0 \quad \forall x, y \in \mathbb{Z}_n$

2. $xy + x(-y) = (-x)y = -(xy) \quad \forall x, y \in \mathbb{Z}_n$

$xy + (-x)y = (x + (-x))y = 0y = 0$

$\Rightarrow -xy = -x(y) = (-x)y$

Tương tự: $x(-y) + xy = (-y + y)x = 0x = 0$

$\Rightarrow x(-y) = -xy$

$\Rightarrow (-x)y = x(-y) = -xy \quad \forall x, y \in \mathbb{Z}_n$

3. $(-x)(-y) = xy \quad \forall x, y \in \mathbb{Z}_n$

Câu 2 đã C/m: $(-x)y = x(-y)$

Và có: $(-x)(-y) = x(-(-y)) = xy$

$\Rightarrow (-x)(-y) = xy \quad \forall x, y \in \mathbb{Z}_n$

BT



$$4. x(y-z) = xy - xz, (y-z)x = yx - zx \quad \forall x, y, z \in \mathbb{Z}_n$$

$$\text{Ta có theo câu 2: } x(y-z) = x(y + (-z))$$

$$= xy + x(-z) = xy - xz$$

$$\text{Tương tự: } (y-z)x = (y + (-z))x = yx - zx$$

\Rightarrow ĐPCM

$$5. x(ny) = n(xy) = (nx)y \quad \forall x, y \in \mathbb{Z}_n$$

$$* n = 0 \Rightarrow \text{ĐPCM câu 1} \quad (1)$$

$$* n \in \mathbb{Z}_n: n(xy) = xy + xy + \dots + xy$$

$$= x \underbrace{(y + \dots + y)}_n = x(ny)$$

$$= \underbrace{(x + \dots + x)}_n y = (nx)y \quad (2)$$

$$* \text{Nếu } n \neq -k, k \in \mathbb{Z}_n$$

$$n(xy) = -k(xy) = -(k(xy)) =$$

$$= \begin{cases} -(k(xy)) = -(kx)y = (-kx)y = (nx)y \\ -(x(ky)) = x(-ky) = x((-k)y) \end{cases} \quad (3)$$

$$= x(ny)$$

(1)(2)(3) \Rightarrow ĐPCM.