PROGRAMA PROFESIONAL

-

TÍTULO DEL TRABAJO

Tarea - Algoritmo RSA

CURSO

Álgebra Abstracta

Alumnos:

- Royer Diosdado Carcausto Choquehuanca
- Fabricio Arián Messa Mandujano

Grupo: CCOMP3-2

Año: 2022

1. (5 points) Si m es el **mensaje** y c es el **cifrado** (ambos representados por un entero). Y además, la clave pública es $P = \{e, n\}$ (en ese orden). Hallar m cuando:

$$P = \{65537, 999630013489\} \quad y \quad c = 747120213790$$

Cifrado=747120213790

P = { e, n }
e = 65537
n = 999630013489

Según el punto 5: d -> ed = 1 mod ϕn ⟶ Sacamos el inverso multiplicativo de "e" con ϕ n

```python
import math

def euclides(a, b):
    if b == 0:
        return a
    return euclides(b, a % b)

def phi(n):
    r = 0
    for i in range(n):
        d = euclides(i, n)
        if d == 1:
            r = r + 1
    return r

print(phi(999630013489))
```

```
999628013860
```

ϕn = 999628013860 e = 65537

Usamos el Algoritmo Extendido de Euclides y tenemos que la inversa es :

```
C:\Users\iNTEL\AppData\Local\Programs\
755383642193
Press any key to continue . . .
```

d = 755383642193

POR LO TANTO:

$$m = c^{d} \bmod n$$

755383642193

m = 747120213790 mod 999630013489

```python
m = pow(747120213790,755383642193,999630013489)
print(m)
```

```
C:\Users\iNTEL\AppData\Local\Programs\P
100000000001
Press any key to continue . . .
```

2. (7 points) Si m es el `mensaje` y c es el `cifrado` (ambos representados por un entero). Y además, la clave pública es $P = \{e, n\}$ (en ese orden). Hallar m cuando:

$$P = \{7, 35794234179725868774991807832568455403003778024228226193\\ 53290819048467025236467741151351610524716862458319335 44\}$$

$$c = 35794234179725868774991807832568455403003778024228226193\\ 53290819048467025236467741151351605247168624583193354 4$$

Sin embargo al enviar el mismo `mensaje` (m) cuando $e' = 11$, el `cifrado` resulto ser

$$c' = 35794234179725868774991807832568455403003778024228226193\\ 53290819048467025236466578674875982253135244453338818 4.$$

P = { e, n }
e = 7
n =
3579423417972586
8774991807832568
4554030037780242
2822619353290819
0484670252364677
4115135161112045
0406031756866 7

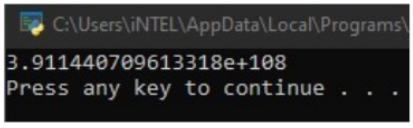
cifrado =
3579423417972586
8774991807832568
4554030037780242
2822619353290819
0484670252364677
4115135160524716
8624583193354 4

Mismo procedimiento del ejercicio 1:

$$\phi n = 1.3690042483646612e + 109$$

e = 7

Usamos nuevamente el Algoritmo Extendido de Euclides para la inversa:



d = 3.9114407096133 18e+108

Por lo tanto:

$$m = c^{d} \bmod n$$