

## 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

"El alumno declara haber realizado el presente trabajo de acuerdo a las normas de la Universidad Católica San Pablo" 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:

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

P = { e, n }

Cifrado=747120213790

e = 65537

n = 999630013489

Según el punto 5:  $d \rightarrow ed = 1 \mod \Phi n$  Sacamos el inverso multiplicativo de "e" con  $\Phi n$ 

e = 65537

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



d = 755383642193

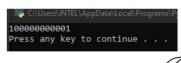
POR LO TANTO:

 $m = c^d \mod n$ 

m = 747120213790 755383642193

mod 999630013489

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



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:

$$\begin{split} P = & \{7,357942341797258687749918078325684554030037780242282261\\ & 93532908190484670252364677411513516111204504060317568667\}\\ c = & 35794234179725868774991807832568455403003778024228226193\\ & 532908190484670252364677411513516052471686245831933544 \end{split}$$

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

 $c' = 357942341797258687749918078325684554030037780242282261935329081 \\90484670252364665786748759822531352444533388184.$ 

P = { e, n } e = 7 n = 35794234179725868 77499180783256845 5403003778024228 22619353290819048 467025236467741151 3516111204504060317 568667

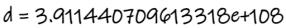
cifrado =
35794234179725868
77499180783256845
5403003778024228
22619353290819048
467025236467741151
35160524716862458
31933544

Mismo procedimiento del ejercicio 1:

$$\phi N = 1.3690042483646612e + 109$$
 $e = 7$ 

Usamos nuevamente el Algoritmo Extendido de Euclides para la inversa: 3.911440709613318e+108







Por lo tanto:

