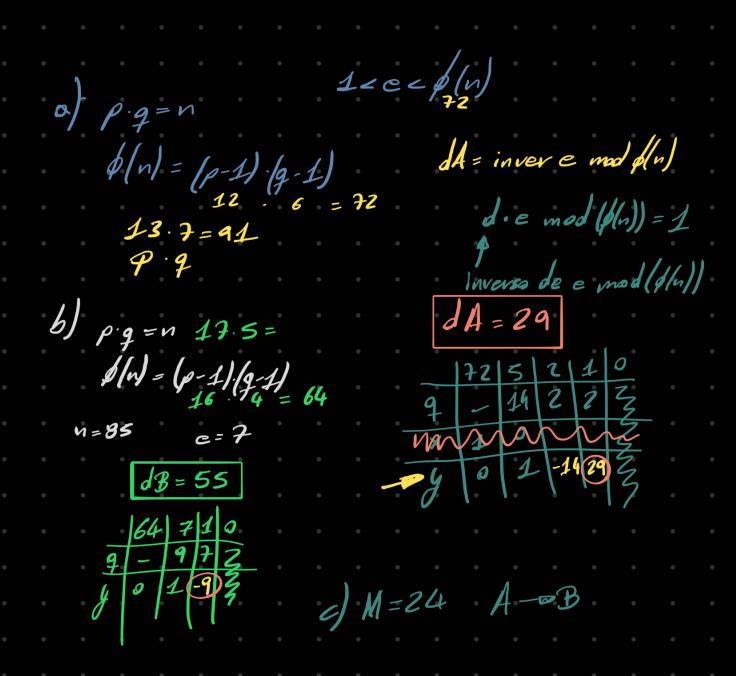
Ejercicio 1. Adela (A) y Benito (B) tienen como clave pública RSA: nA = 91, eA = 5; nB = 85, eB = 7.

- a) Encuentra la clave privada dA de Adela (A).
- b) Encuentra la clave privada dB de Benito (B).
- c) Cifra el mensaje numérico M = 24 que Adela (A) envía confidencialmente a Benito (B)
- d) Firma el hash numérico h(M) = 10 que Benito (B) envía a Adela (A).



242 mad (85) =

Ejercicio 2. Claves RSA del sistema:

Amparo (A) =
$$nA = 187$$
; $eA = 3$

Deberás usar el algoritmo extendido de Euclides y el algoritmo de exponenciación rápida. Se pide:

- a) Enguentra la clare privada de Amparo de 160 3 1 0
- b) Encuentra la clave priyada Bartolo dB. q
- c) Amparo envía confidencialmente el valor 41 a Barto o Calcula el criptogramalrecilate pas B
- la firma de un kash 77 a Ampard. ¿Qué criptograma d) Bartolo envía dA=160-53=107 recibe A. ¿Qué puced (20) = 1

$$\beta(n) = (p-1)(q-1)$$

$$6 - 12 = 72$$
mod

41 mod(91)
$$(415)^{2} \cdot 41 = 6^{2} \cdot 41 = 20$$

hash a encripto con su propio dove privado

$$mod (nB) \qquad 77^{59} \mod (nB) \qquad 77^{59} \mod$$

1.
$$n_{A}=209$$
 $e_{A}=7$
 dA ?

 $f: q=209$
 $f: q=209$

2.
$$K=85$$
 $K=85$
 $K=85$

$$X = \frac{\ln 65}{13}$$

$$X = \frac{\ln 65}{100}$$

$$X = \frac{\ln 65}{$$

Tamaño de bloque? 3 byte 3x8 = 24 2 30

HOL 01000111 01001101 01001010

AAM 1000001 1000001 1001011

TGO 1001000 1000110 1001101

72 70 79

72 79 76

01001000 01001111 01001100