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).

a) $p \cdot q = n$

$1 < e < \phi(n)$, $\phi(n) = 72$

$\phi(n) = (p-1)\cdot(q-1)$

$12 \cdot 6 = 72$

$13 \cdot 7 = 91$

$p \cdot q$

$dA = \text{inverse } e \bmod \phi(n)$

$d \cdot e \bmod(\phi(n)) = 1$

↑ inverso de e mod($\phi(n)$)

$dA = 29$

	72	5	2	1	0
q	–	14	2	2	
m	1	0			
y	0	1	-14	29	

b) $p \cdot q = n$ $17 \cdot 5 =$

$\phi(n) = (p-1)\cdot(q-1)$

$16 \cdot 4 = 64$

$n = 85$ $e = 7$

$dB = 55$

	64	7	1	0
q	–	9	7	
y	0	1	-9	

c) $M = 24$ $A \rightarrow B$

$24^7 \bmod(85) =$

Ejercicio 2. Claves RSA del sistema:
Amparo (A) = nA = 187; eA = 3
Bartolo (B) son: nB = 91; eB = 11.
Deberás usar el algoritmo extendido de Euclides y el algoritmo de exponenciación rápida.Se pide:
a) Encuentra la clave privada de Amparo dA
b) Encuentra la clave privada Bartolo dB.
c) Amparo envía confidencialmente el valor 41 a Bartolo. Calcula el criptograma recibido por B.
d) Bartolo envía la firma de un hash 77 a Amparo. ¿Qué criptograma recibe A. ¿Qué sucede?

a) d_A? $n_A = 187$ $e_A = 3$

$p \cdot q = 187$ $11 \cdot 17 = 187$

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

$10 \cdot 16 = 160$

$d_A \cdot 3 \bmod(160) = 1$

	160	3	1	0
q	—	53	3	2
y	0	1	-53	

$d_A = 160 - 53 = 107$

b) d_B? $n_B = 91$ $e_B = 11$

$p \cdot q = 91$ $7 \cdot 13 = 91$

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

$6 \cdot 12 = 72$ mod

$11 \cdot d_B \bmod(72) = 1$

	72	11	6	5	1	0
q	—	6	1	1	5	2
y	0	1	-6	7	-13	

$d_B = 72 - 13 = 59$

c) $A \xrightarrow{n_B\ e_B} B$

$M = 41$

$41^{11} \bmod(91)$

$(41^5)^2 \cdot 41 = 6^2 \cdot 41 = 20$

d) hash → encripta con su propia clave privada

$77^{d_B} \bmod(n_B)$ $77^{59} \bmod(91)$

$77^{50} \cdot 77^9 = (77^5)^{10} \cdot (77^3)^3 = 77^{10} \cdot 77^3 =$

$(77^2)^5 \cdot 77 = 77^2 \cdot 77 = 77$

1. $n_A = 209 \quad e_A = 7$

d_A?

$p \cdot q = 209$

$19 \cdot 11 = 209$

	180	7	5	2	1	0
7	–	25	1	2	2	ξ
y	0	1	-25	26	-77	ξ

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

$18 \cdot 10 = 180$

$\boxed{d_A = 180 - 77 = 103}$

2. $K = 85 \qquad K^{e_A} \bmod (n_A)$

$\boxed{85^7 \bmod (209) = 156}$

$85^5 \cdot 85^2$

$\underbrace{85^2}_{119} \cdot \underbrace{85^3}_{83} \cdot \underbrace{85^2}_{119}$

$= 65$

$X^{77} \bmod (119) = 65$

$77 \cdot \ln X = \ln 65$

$\ln x = \frac{\ln 65}{77}$

$X = e^{\frac{\ln 65}{77}} = 1'05570926$

$X^{13} \bmod (77) = \text{“!!”}$

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

$24048 \cdot 32058 = 7'709\,30784 \cdot 10^8$

$d \cdot e \bmod (\phi(n)) = 1$

	$7'709\,30784 \cdot 10^8$	154 186 157	154 186 156	1	0
q	—	4	1	154	186
y	0	1	-4	S	

Tamaño de bloque? 3 byte $3 \times 8 = 24 < 30$

HOL	01000111	01001101	01001100
AAM	1000001	1000001	1001011
IGO	1001000	1000110	1001101
	72	70	79

72 79 76

01001000 01001111 01001100