

Algoritmo de Potenciación Modular

Para calcular 3^{14} módulo 11

$$(a = 3, b = 14, n = 11)$$

Se calcula la expresión de b en base 2

$$14 = 1110_2$$

<div>valores de a</div> <div>↓</div> $a_{i+1} := a_i^2 \text{ módulo } 11$	a	b	m	valores de m
	3	0	1	↓
	9	1	1	Si $b_i = 0$ entonces
	4	1	9	$m_{i+1} := m_i$
	5	1	3	Si $b_i = 1$ entonces
			4	$m_{i+1} := a_i \cdot m_i \text{ módulo } 11$

3^{14} módulo 11 vale 4

$\mathcal{A} = \text{“aábcdeéfgghiíjklmnñoópqrstuúvwxyzAÁBCDEÉFGHIÍJKLMNÑOÓPQR}$
 $\text{STUÚVWXYZ0123456789 ,.-()”}$

(alfabeto con 81 símbolos)

De Texto a Número Entero

“bala” codificación numérica $[2, 0, 14, 0]$

$[2, 0, 14, 0]$ se corresponde con el número entero

$$2 \cdot 81^3 + 0 \cdot 81^2 + 14 \cdot 81^1 + 0 \cdot 81^0 = 1064016$$

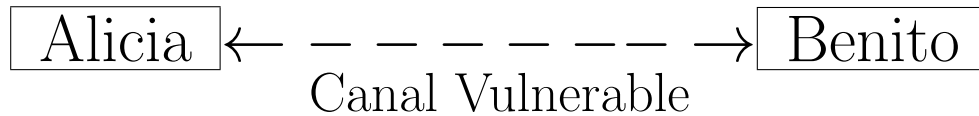
De Número Entero a Texto

para el entero 100, se calculan sus dígitos en base 81

$$[1, 19]$$

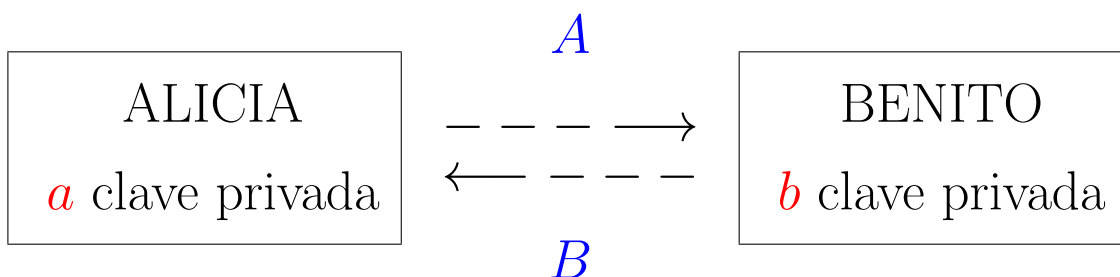
$[1, 19]$ se corresponde con el texto “áo”

Intercambio de Clave de Diffie-Hellman



Eligen un número primo p grande (público).
Calculan g una raíz primitiva módulo p .

- Alicia elige un número a con $0 \leq a \leq p - 2$.
- Alicia envía a Benito, $A := g^a$ módulo p .
- Benito elige un número b con $0 \leq b \leq p - 2$.
- Benito envía a Alicia, $B := g^b$ módulo p .
- La clave que van a compartir es $K := g^{ab}$ módulo p



Alicia calcula
 B^a módulo p

↓
 K

Benito calcula
 A^b módulo p

↓
 K