# Práctica 07: Algoritmos para el protocolo de Diffie-Hellman

lunes 29 de abril de 2019

Apellidos: ..... Nombre: .....

Apellidos: ..... Nombre: .....

Grupo: .....

**AVISO:** Todos los datos los podéis encontrar en el archivo *datos_07_lunes*.

**1. Algoritmo de potenciación modular.** Calcular la potencia modular

$$a^b \text{ módulo } n$$

potencia modular

133342693831

**2. Números enteros codificados como texto y viceversa.**

*a*) Calcular la expresión del número entero $M = 987654321987654321$ en base 81 (escribir los dígitos de dicha expresión en formato lista, de derecha a izquierda).

base 81

$$[6, 46, 80, 61, 60, 16, 46, 14, 36, 36]$$

*b*) Calcular el número entero cuyos dígitos en base 81 vienen dados en la lista

$$[1, 45, 76, 74, 79, 22, 78, 52, 72].$$

número entero

290420192904201 9

*c*) A cada texto escrito en el alfabeto $\mathcal{A}$

$\mathcal{A}$ = "aábcdeéfghiíjklmnñoópqrstuúvwxyzAÁBCDEÉFGHIÍJKLMNÑOÓPQR STUÚVWXYZ0123456789 ,.:-()"

(alfabeto con 81 símbolos), le vamos a asignar un número entero de la siguiente forma:

1) Utilizamos la codificación numérica que a cada símbolo $\alpha$ del alfabeto le asigna el número $n(\alpha) = p(\alpha) - 1$, donde $p(\alpha)$ es la posición que ocupa $\alpha$ dentro del alfabeto. La codificación de un texto será la lista de posiciones. Por ejemplo, el texto "bala" pasa a ser la lista $[2, 0, 14, 0]$.
2) Los datos de la lista anterior se pueden ver como dígitos de la expresión de un número entero en base el cardinal del alfabeto. Por convenio vamos a leer los dígitos de derecha a izquierda. Es decir, para la lista $[2, 0, 14, 0]$ y el alfabeto con 81 símbolos, el entero correspondiente es $2 \cdot 81^3 + 14 \cdot 81 = 1064016$.

Calcular el entero que se corresponde con el texto "29 de abril".

número entero

813500045345754028904

Obtener el texto que se corresponde con el entero 100475755307496626.

texto

Rocinante

**3**. **Protocolo de Diffie-Hellman.** Supongamos que Alicia y Benito utilizan el protocolo de intercambio de claves de Diffie-Hellman, con número primo $p$ y generador multiplicativo $g = 2$ (raíz primitiva módulo $p$). Los datos de las claves parciales se envían en formato texto (usando el sistema de codificación que pasa de número entero a texto, descrito en el apartado anterior) a través de un canal vulnerable. Se sabe que Alicia envía a Benito el texto

écxÓFTl vsRÍO6Ñ1

y que Benito envía a Alicia el texto

dpé:IsIvÑD75mmW,

Sabiendo que la clave privada que usó Alicia fue $a = 2904201929042019$, ¿cuál es la clave compartida que han acordado Alicia y Benito?

clave compartida

áiU7k:1x SAw)Gny