

Práctica 07: Algoritmos para el protocolo de Diffie-Hellman

miércoles 24 de abril de 2019

APELLIDOS: NOMBRE:

APELLIDOS: NOMBRE:

GRUPO:

AVISO: Todos los datos los podéis encontrar en el archivo *datos_07_miercoles*.

1. Algoritmo de potenciación modular. Calcular la potencia modular

a^b módulo n

potencia modular

101400389190

2. Números enteros codificados como texto y viceversa.

- a) Calcular la expresión del número entero $M = 123456789123456789$ en base 81 (escribir los dígitos de dicha expresión en formato lista, de derecha a izquierda).

base 81

[66, 50, 48, 17, 26, 45, 41, 33, 63]

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

[1, 24, 7, 46, 30, 48, 79, 51, 53].

número entero

2404201924042019

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

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

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

- 1) Utilizamos la codificación numérica que a cada símbolo α del alfabeto le asigna el número $n(\alpha) = p(\alpha) - 1$, donde $p(\alpha)$ es la posición que ocupa α 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 “24 de abril”.

número entero
812749572169269033299

Obtener el texto que se corresponde con el entero 1000000.

texto
á7ÁS

- 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

“bú32a4Í2lDíhUeÉB”

y que Benito envía a Alicia el texto

“áuÁTJKWz7É I.Ñ2É”

Sabiendo que la clave privada que usó Benito fue $b = 1717171717171717$, ¿cuál es la clave compartida que han acordado Alicia y Benito?

clave compartida
gXó.CYCfeFHMOs16