

## Práctica 08: Sistemas Criptográficos Mixtos

lunes 6 de mayo de 2019

APELLIDOS: ..... NOMBRE: .....

APELLIDOS: ..... NOMBRE: .....

GRUPO: .....

**AVISO:** Todos los datos los podéis encontrar en el archivo *datos\_08\_lunes*.

Supongamos que tenemos un sistema criptográfico donde los mensajes se cifran usando el sistema de clave privada de Vigenère y la clave privada utilizada es intercambiada por los usuarios vía el protocolo de Diffie-Hellman (sólo podemos acordar la clave por el canal, y el canal no es seguro). El proceso de cifrado es el siguiente:

- Primero los dos usuarios utilizan Diffie-Hellman para acordar la clave  $K$ .
- A continuación, cifran sus mensajes usando Vigenère con clave  $K$ .

**CASO PRÁCTICO:** Alicia y Benito son usuarios del sistema y escriben sus mensajes en el alfabeto

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

(alfabeto con 81 símbolos). Utilizan el protocolo de intercambio de claves de Diffie-Hellman, con número primo  $p$  y generador multiplicativo  $g = 3$  (raíz primitiva módulo  $p$ ). Los datos de las claves parciales las envían en formato texto a través del canal vulnerable. Se sabe que Alicia envía a Benito el texto

cl)jEoÉGjíSki

y Benito envía a Alicia el texto

h)L-zceJ(m,iLn

A continuación cifran todos sus mensajes usando Vigenère con clave de cifrado la obtenida por Diffie-Hellman.

Se pide descifrar el mensaje cifrado indicado en el archivo *datos\_08\_lunes*, sabiendo que la clave privada que usó Alicia para realizar Diffie-Hellman fue

$$a = 63336484957353$$

mensaje en claro

Me gustas cuando callas porque estás como ausente,  
y me oyes desde lejos, y mi voz no te toca.

Parece que los ojos se te hubieran volado  
y parece que un beso te cerrara la boca.

Poema 15. Pablo Neruda (Chile, 1904)

**AVISO:** Para escribir el mensaje en claro tenéis que considerar los dos espacios como un cambio de línea.