Práctica 08: Sistemas Criptográficos Mixtos

miércoles 8 de mayo de 2019

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

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

Grupo: .....

AVISO: Todos los datos los podéis encontrar en el archivo *datos_08_miercoles*.

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

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

(alfabeto con 81 símbolos). Utilizan el protocolo de intercambio de claves de Diffie-Hellman, con número primo p y generador multiplicativo $g = 10$ (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

íyr5IR6ípDSAúY

y Benito envía a Alicia el texto

eXPKeSítÍííDN,

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_miercoles*, sabiendo que la clave privada que usó Alicia para realizar Diffie-Hellman fue

$$a = 63332323232451757353$$

mensaje en claro

YO QUE CREÍ que la luz era mía
precipitado en la sombra me veo.
Ascua solar, sideral alegría
ígnea de espuma, de luz, de deseo.
(ETERNA SOMBRA, Miguel Hernández, 1910-1942)

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