# Tarea 02

miércoles 22 de mayo

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

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

Grupo .....

Alicia y Benito son usuarios de un sistema de comunicación donde escriben sus mensajes en el alfabeto

$$\mathcal{A} = \text{“abcdefghijklmnñopqrstuvwxyzáéíóú ,.ABCDEFGHIJKLMNÑOPQRSTUVWXYZ”},$$

y usan 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.

1. Alicia quiere mandarle a Benito la frase “Estamos comenzando la última tarea.”, cifrada con Vigenère y clave de cifrado “Mucha suerte”. Calcular el mensaje cifrado que envía a Benito.

   (2 puntos)

   mensaje cifrado

   “xFvhmMDRg, iYMctdMP eOPofíñh QsEirS”

2. Benito responde a Alicia con el mensaje cifrado

   “EUPákfUágcFuakíIágUPíFkCXkíIáY”

   Sabiendo que para cifrarlo usó el cifrado de sustitución monoalfabética con clave $(27, 10)$, descifrar dicho mensaje (2 puntos)

   mensaje en claro

   “Mensajes cifrados endiablados.”

3. Ahora necesitan acordar una clave usando el sistema criptográfico de Diffie-Hellman, para ello usan el número primo $p = 131414242343537725243372873$ y el generador $g = 10$. Se conocen las clave privadas de Alicia $a = 123456789123456$ y de Benito $b = 987654321987654$.

   *a*) ¿Que mensaje le manda Alicia a Benito?

   (2 puntos)

   mensaje enviado

   “cLAókwHéxChWZCé”

   *b*) ¿Cuál es la clave compartida?

   (2 puntos)

   clave compartida

   “fyyx JlnnmATKkQ”

4. Los dos son usuarios del RSA por bloques. Alicia tiene clave pública ($n_A = 26857579751332888463, e_A = 15625$) donde $n_A = 5182429907 \cdot 5182429909$ y Benito tiene clave pública ($n_B = 91549193550412679, e_B = 2021$) donde $n_B = 1282493 \cdot 71383776403$.

   *a*) Si Benito recibe de Alicia el mensaje cifrado

   "epDesZWUucbVPHczYiEúbrRvRgAWHggkkÑíVCñGScFñednáKól"

   obtener el mensaje en claro.

   (2 puntos)

   mensaje en claro

   "Benito, he recibido tu clave y todo me encaja"

   *b*) Si Alicia quiere enviar a Benito la frase

   "Ya tengo la clave compartida fyyx JlnnmATKkQ."

   ¿Qué mensaje cifrado le debe enviar?

   (2.5 puntos)

   mensaje cifrado

   "ezUuíYaíéraFlqPkYBcNgxótÑNlFJheúpahBéjíSeRJOxlQKíf"

   *c*) Si Benito quiere enviar a Alicia un mensaje en claro de longitud 74580, ¿Que longitud tendrá el mensaje cifrado? (Explicar el resultado obtenido)

   (2.5 puntos)

   longitud del mensaje cifrado

   La longitud del bloque para cifrar los mensajes y enviárselos a Alicia es de 11 caracteres. Por lo tanto, tendremos que cifrar 6780 bloques del mensaje en claro y obtendremos 6780 bloques cifrados, cada uno de ellos con longitud 12. Por lo tanto, la longitud del mensaje cifrado será de 81360 caracteres.