# Tarea 02

lunes 20 y martes 21 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 terminando las prácticas.”, cifrada con Vigenère y clave de cifrado “Murciélago”. Calcular el mensaje cifrado que envía a Benito.

   (2 puntos)

   mensaje cifrado

   “xFDctIó zsd,zoiGñoDzMFOrzTntñqMFQ”

2. Benito responde a Alicia con el mensaje cifrado

   “,nkdCuOeLNUtdLUuVOLVekOekNLkg”

   Sabiendo que para cifrarlo usó el cifrado de sustitución monoalfabética con clave $(9, 10)$, descifrar dicho mensaje (2 puntos)

   mensaje en claro

   “Cuando terminemos esta tarea.”

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 $a = 12345678912345$ y de Benito $b = 98765432198765$.

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

   (2 puntos)

   mensaje cifrado

   “kbOóhSVUvPtéTLá”

   *b*) ¿Cuál es la clave compartida?

   (2 puntos)

   clave compartida

   “fílBAeVúkMACxIM”

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 Alicia recibe de Benito el mensaje cifrado

   "mbOXúñAXsu,í amwuanXrlñIMZ,MNXúqd"

   obtener el mensaje en claro.

   (2 puntos)

   mensaje en claro

   "Alicia, he recibido tu clave.."

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

   "Ya tengo la clave compartida.."

   ¿Qué mensaje cifrado le debe enviar?

   (2.5 puntos)

   mensaje cifrado

   "oá AgiKEéIqjUFJFcJRxAteXhYsCháyMM"

   *c*) Si Alicia quiere enviar a Benito un mensaje en claro de longitud 74230, ¿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 Benito es de 10 caracteres. Por lo tanto, tendremos que cifrar 7423 bloques del mensaje en claro y obtendremos 7423 bloques cifrados, cada uno de ellos con longitud 11. Por lo tanto, la longitud del mensaje cifrado será de 81653 caracteres.