Grupo 10	Ejemplo Primer Control de Seguretat Informàtica	Q1: 04-10-2019
Nombre:	Apellidos:	

Test. 3 puntos.
Tiempo de resolución estimado: **20 minutos**
Las preguntas pueden ser

- Respuesta única (RU). Una respuesta RU correcta cuenta 0.3 puntos.
- Multirespuesta (MR). Una respuesta MR correcta cuenta 0.3 puntos, la mitad si hay un solo error, 0 en los otros casos. En las MR puede haber desde una hasta todas respuestas correctas.

1. **MR**. Marca la o las afirmaciones correctas

- ☒ AES es un sistema de cifrado simétrico
- ☐ DES es un sistema de cifrado asimétrico
- ☒ DES es un sistema de cifrado en bloques
- ☐ AES es un sistema de cifrado por flujo

2. **MR**. Para la firma digital

- ☐ Se puede usar DES
- ☐ Se puede usar AES
- ☒ Se puede usar RSA
- ☐ Se puede usar OTP

3. **RU**. El principio de difusión de Shannon …

- ☐ es el que consigue que con un pequeño cambio en la clave haya un gran cambio en el texto cifrado
- ☒ es el que consigue que un pequeño cambio en el texto en claro provoque un gran cambio en el texto cifrado
- ☐ es el que consigue que la relación entre la clave e el mensaje cifrado sea la más compleja
- ☐ es el que dice que el algoritmo de cifrado debe ser publico y la clave secreta

4. **RU**. Indicar a que sirve el algoritmo de Diffie-Hellman

- ☐ A cifrar un texto usando una clave publica en la criptografía asimétrica
- ☐ A intercambiar un texto a través de un canal no seguro
- ☐ Para verificar que la firma digital en un documento es autentica
- ☒ Para determinar una clave secreta en la criptografía simétrica usando un canal no seguro y sin la necesidad de enviarse esta clave

5. **RU**. En un mensaje cifrado enviado por A a B en la criptografía asimétrica

- ☐ A usa la clave privada de B para cifrar un mensaje
- ☐ B usa la clave publica de A para descifrar el mensaje de A
- ☐ B usa la clave privada de A para descifrar el mensaje de A
- ☒ B usa la clave privada de B para descifrar el mensaje de A

6. **RU**. En un documento firmado digitalmente por A

- ☐ Si B quiere autentificar la firma, debe usar la clave privada de A
- ☒ A ha firmado usando su clave privada
- ☐ A ha firmado usando su clave publica
- ☐ Si el documento es para B, A debe firmar usando la clave publica de B

7. **MR**. Marca la o las afirmaciones correctas

- ☒ RSA es un algoritmo de cifrado usando en criptografía asimétrica
- ☒ ElGamal es un algoritmo de cifrado usando en criptografía asimétrica
- ☒ 3DES es un algoritmo de cifrado usando en criptografía simétrica
- ☐ OTP es un ejemplo de cifrado asimétrico

8. **RU**. Indicar a que sirve el cifrado por flujo

- ☒ Para cifrar incrementalmente un mensaje convirtiendo el texto en claro en uno cifrado bit a bit
- ☐ Para cifrar bloques de mensajes de tamaño fijos y enviarlos a través de un flujo de paquetes
- ☐ Para crear claves secretas que vayan cambiando en tiempo real según vaya avanzando el envío de mensajes
- ☐ Por ejemplo, se usa en AES para permutar y mezclar en varias rondas seguidas flujos de mensajes y claves secretas

9. PKI

10. PKI

Grupo 10	Ejemplo Primer Control de Seguretat Informàtica	Q1: 04-10-2019
Nombre:	Apellidos:	

Problemas. 7 puntos.
Tiempo de resolución estimado: **35 minutos**.

1) Tiempo de resolución estimado: **10 minutos**
Alice y Bob quieren usar una clave privada para crear un canal seguro usando criptografía DES
Contestar a estas preguntas.

a) Determinar que método pueden usar para compartir una clave privada de forma segura y describir como funciona.

El metodo Diffie-Helman
Los usuarios A y B eligen un grupo cíclico finito de orden n y un generador α menor de n.
A elige un número a menor de n y calcula $w = \alpha^a \bmod n$ y envía este resultado a B.
B elige un número b menor de n y calcula $z = \alpha^b \bmod n$ y envía este resultado a A.
A recibe z y calcula $z^a \bmod n = X$.
B recibe w y calcula $w^a \bmod n = X$. X es la clave privada

b) Alice y Bob eligen un grupo cíclico finito G de 29 y un generador $\alpha = 2$. Luego, Alice elige el número 5 y Bob elige el número 12. Describe que valores se intercambian Alice y Bob y que clave privada usaran.

Alice calcula $2^5 \bmod 29 = 3$ y envía 3 a Bob
Bob calcula $2^{12} \bmod 29 = 7$ y envía 7 a Alice
Alice calcula $7^5 \bmod 29 = 16$
Bob calcula $3^{12} \bmod 29 = 16$
16 será la clave privada

2) Tiempo de resolución estimado: **15 minutos**
Alice quiere usar ElGamal para recibir mensaje privados de Bob. Deciden usar el grupo cíclico finito G de 23 y un $\alpha = 11$.
Contestar a las siguientes preguntas

a) Alice elige a = 6 como clave privada. Ayuda Alice a calcular su clave publica

$\alpha^a \in G = 11^6 \bmod 23 = 9$
Alice envía a Bob la clave publica (11, 23, 9)

b) Bob quiere enviar el mensaje m = 10 a Alice y elige el número b = 3. Ayuda Bob a calcular el mensaje cifrado c

$\alpha^b \in G = 11^3 \bmod 23 = 20$
$c = m \cdot (\alpha^a)^b \in G = 10 \cdot 9^3 \bmod 23 = 22$
Bob envía a Alice el mensaje (20, 22)

c) Ayuda Alice a descifrar el mensaje

$x = (\alpha^b)^a \in G = 20^6 \bmod 23 = 16$
$x^{-1} \in G = 16^{-1} \bmod 23 = 13$
$m = c \cdot x^{-1} \in G = 22 \cdot 13 \bmod 23 = 10$

3) Tiempo de resolución estimado: **10 minutos**
Alice ha usado RSA para determinar su clave publica y su clave privada. En concreto, ha usado p = 17, q = 23 y e =13. Contesta a las siguientes preguntas.

a) Calcula la clave privada de Alice

$n = p \cdot q = 391$
$\phi(n) = (p-1)(q-1) = 352$
$d = e^{-1} \bmod \Phi(n) = 13^{-1} \bmod 352$

$352 = 13 \times 27 + 1$
$1 = 352 - 27 \times 13$
$1 \bmod 352 = (352 \bmod 352) + (-27 \times 13 \bmod 352) \rightarrow$
$1 = -27 \times 13 \bmod 352 \rightarrow$
$1 = (352 - 27) \times 13 \bmod 352 \rightarrow 1 = 325 \times 13 \bmod 352$
$325 = 13^{-1} \bmod 352$
$d = 325$

Clave publica = (391, 13)
Clave privada = (391, 325)

b) Bob quiere enviar el mensaje 11 a Alice, calcula el mensaje cifrado que recibirá Alice

$c = m^e \bmod n = 11^{13} \bmod 391 = 109$

$13 \rightarrow z = 1101$

$x = 1^2 \bmod 391$
$z_0 = 1 \rightarrow x = 11 \times 1 \bmod 391 = 11$

$x = 11^2 \bmod 391 = 121$
$z_1 = 1 \rightarrow x = 11 \times 121 \bmod 391 = 158$

$x = 158^2 \bmod 391 = 331$
$z_2 = 0 \rightarrow x = 331$

$x = 331^2 \bmod 391 = 81$
$z_3 = 1 \rightarrow x = 11 \times 81 \bmod 391 = 109$

$c = 109$