

Grupo 10	Ejemplo Primer Control de Seguridad Informática	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.

<p>1. MR. Marca la o las afirmaciones correctas</p> <p><input type="checkbox"/> AES es un sistema de cifrado simétrico</p> <p><input type="checkbox"/> DES es un sistema de cifrado asimétrico</p> <p><input type="checkbox"/> DES es un sistema de cifrado en bloques</p> <p><input type="checkbox"/> AES es un sistema de cifrado por flujo</p>	<p>2. MR. Para la firma digital</p> <p><input type="checkbox"/> Se puede usar DES</p> <p><input type="checkbox"/> Se puede usar AES</p> <p><input type="checkbox"/> Se puede usar RSA</p> <p><input type="checkbox"/> Se puede usar OTP</p>
<p>3. RU. El principio de difusión de Shannon ...</p> <p><input type="checkbox"/> es el que consigue que con un pequeño cambio en la clave haya un gran cambio en el texto cifrado</p> <p><input type="checkbox"/> es el que consigue que un pequeño cambio en el texto en claro provoque un gran cambio en el texto cifrado</p> <p><input type="checkbox"/> es el que consigue que la relación entre la clave e el mensaje cifrado sea la más compleja</p> <p><input type="checkbox"/> es el que dice que el algoritmo de cifrado debe ser publico y la clave secreta</p>	<p>4. RU. Indicar a que sirve el algoritmo de Diffie-Hellman</p> <p><input type="checkbox"/> A cifrar un texto usando una clave publica en la criptografía asimétrica</p> <p><input type="checkbox"/> A intercambiar un texto a través de un canal no seguro</p> <p><input type="checkbox"/> Para verificar que la firma digital en un documento es autentica</p> <p><input type="checkbox"/> Para determinar una clave secreta en la criptografía simétrica usando un canal no seguro y sin la necesidad de enviarse esta clave</p>
<p>5. RU. En un mensaje cifrado enviado por A a B en la criptografía asimétrica</p> <p><input type="checkbox"/> A usa la clave privada de B para cifrar un mensaje</p> <p><input type="checkbox"/> B usa la clave publica de A para descifrar el mensaje de A</p> <p><input type="checkbox"/> B usa la clave privada de A para descifrar el mensaje de A</p> <p><input type="checkbox"/> B usa la clave privada de B para descifrar el mensaje de A</p>	<p>6. RU. En un documento firma digitalmente por A</p> <p><input type="checkbox"/> Si B quiere autentificar la firma, debe usar la clave privada de A</p> <p><input type="checkbox"/> A ha firmado usando su clave privada</p> <p><input type="checkbox"/> A ha firmado usando su clave publica</p> <p><input type="checkbox"/> Si el documento es para B, A debe firmar usando la clave publica de B</p>
<p>7. MR. Marca la o las afirmaciones correctas</p> <p><input type="checkbox"/> RSA es un algoritmo de cifrado usando en criptografía asimétrica</p> <p><input type="checkbox"/> ElGamal es un algoritmo de cifrado usando en criptografía asimétrica</p> <p><input type="checkbox"/> 3DES es un algoritmo de cifrado usando en criptografía simétrica</p> <p><input type="checkbox"/> OTP es un ejemplo de cifrado asimétrico</p>	<p>8. RU. Indicar a que sirve el cifrado por flujo</p> <p><input type="checkbox"/> Para cifrar incrementalmente un mensaje convirtiendo el texto en claro en uno cifrado bit a bit</p> <p><input type="checkbox"/> Para cifrar bloques de mensajes de tamaño fijos y enviarlos a través de un flujo de paquetes</p> <p><input type="checkbox"/> Para crear claves secretas que vayan cambiando en tiempo real según vaya avanzando el envío de mensajes</p> <p><input type="checkbox"/> Por ejemplo, se usa en AES para permutar y mezclar en varias rondas seguidas flujos de mensajes y claves secretas</p>
<p>9. PKI</p>	<p>10. PKI</p>

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.

- 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.

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

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

- c) Ayuda Alice a descifrar el mensaje

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

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