Grupo 10	Primer Control de Seguretat Informàtica	Q1: 11-10-2019
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

- ☐ Generalmente el algoritmo de cifrado es secreto y el de descifrado es publico
- ☐ Los algoritmos de cifrado y descifrado son secretos en la criptografía simétrica, mientras que son públicos en la criptografía asimétrica
- ☒ La clave común entre los dos extremos es secreta en la criptografía simétrica
- ☐ En la criptografía asimétrica, se usa un algoritmo de cifrado publico y uno privado

2. **RU**. Según el criterio de Shannon, un cifrado debería garantizar

- ☐ Distribución y privacidad
- ☐ Confidencialidad e integridad
- ☐ Difusión y autenticidad
- ☐ Autenticidad y unicidad
- ☐ Privacidad e integridad
- ☒ Confusión y difusión
- ☐ Confidencialidad y autenticidad
- ☐ Distribución y confusión

3. **MR**. Una clave secreta en un cifrado simétrico se puede intercambiar entre los usuarios A y B…

- ☐ cifrando la clave con la clave misma
- ☒ usando el algoritmo de Diffie-Helmann
- ☐ si A envía a B la clave secreta cifrada con la clave privada de A y B descifra con la clave pública de A
- ☐ usando el algoritmo de ElGamal

4. **RU**. Si Alex quiere verificar que Bárbara ha firmado un documento digitalmente

- ☐ Alex debe conocer la función de Hash que ha usado Bárbara y la clave privada de Bárbara
- ☐ Alex solo necesita la clave pública de Bárbara
- ☐ Alex solo necesita la clave privada de Bárbara
- ☒ Alex debe conocer la función de Hash que ha usado Bárbara y la clave pública de Bárbara

5. **MR**. El algoritmo ElGamal

- ☐ Es usado para la firma digital
- ☒ Se puede usar para cifrar una clave privada en la criptografía hibrida
- ☒ Permite generar una clave publica y una privada en criptografía asimétrica
- ☐ Usa varias rondas de permutaciones y mezclas entre un texto y la clave privada

6. **MR**. El objetivo principal de la criptografía es proteger

- ☒ La confidencialidad, integridad y disponibilidad de los datos
- ☒ La reputación
- ☐ La unicidad y fiabilidad de los datos
- ☒ Los recursos
- ☐ La autenticidad, encriptación y certificación de los datos
- ☐ La repercusión

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

- ☒ OTP usa claves secretas aleatorias de un único uso
- ☒ AES es un algoritmo de cifrado simétrico en bloques
- ☐ RSA es un algoritmo de cifrado de flujo
- ☐ Diffie-Helmann es un algoritmo de cifrado asimétrico

8. **MR**. En la ciberseguridad

- ☒ Existen normativas nacionales y europeas para que las organizaciones apliquen políticas y protocolos de seguridad
- ☒ Las personas suelen ser el eslabón más débil
- ☒ Hoy en día principalmente está amenazada por el crimen organizado
- ☐ Hoy en día es un problema casi del todo resuelto y ya se destinan menos recursos y dinero

9. **MR**. Indica cuales de siguientes modelos son de confianza en PKI

- ☒ Modelo plano
- ☐ Modelo puro
- ☒ Modelo distribuido
- ☒ Modelo de certificación cruzada jerárquica
- ☒ Modelo de lista de confianza jerárquica

10. **MR**. Indicar cuales de las siguientes son funciones de las Certificate Authority (CA)

- ☒ Firman digitalmente y ponen a disposición un certificado de confianza que asocia una entidad con su clave pública
- ☐ Pueden opcionalmente generar la clave secreta en la criptografía simétrica
- ☒ Certifican la confianza de otras CA
- ☐ Generan una marca de tiempo en los documentos firmados con firma digital

Grupo 10	Primer Control de Seguretat Informàtica	Q1: 11-10-2019
Nombre:	Apellidos:	

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

1) Tiempo de resolución estimado: **10 minutos**
Alex ha usado RSA para determinar su clave publica y su clave privada. En concreto, ha usado p = 37, q = 29 y e = 17. Calcula la clave pública y privada de Alex

$n = p \cdot q = 37 \times 29 = 1073$
$\phi(n) = (p-1)(q-1) = 36 \times 28 = 1008$
$d = e^{-1} \bmod \Phi(n) = 17^{-1} \bmod 1008$

$1008 = 17 \times 59 + 5$ $\quad 17 = 5 \times 3 + 2$ $\quad 5 = 2 \times 2 + 1$
$1 = 5 - 2 \times 2$
$2 = 17 - 3 \times 5 \rightarrow 1 = 5 - 2 \times (17 - 3 \times 5) \rightarrow 1 = 7 \times 5 - 2 \times 17$
$5 = 1008 - 59 \times 17 \rightarrow 1 = 7 \times (1008 - 59 \times 17) - 2 \times 17 \rightarrow 1 = 7 \times 1008 - 415 \times 17$

$1 \bmod 1008 = (7 \times 1008 \bmod 1008) + (-415 \times 17 \bmod 1008) \rightarrow 1 = ((1008 - 415) \times 17) \bmod 1008 \rightarrow$
$\rightarrow 1 = 593 \times 17 \bmod 1008$
$d = 593$

Clave publica = (1073, 17)
Clave privada = (1073, 593)

2) Tiempo de resolución estimado: **10 minutos**
Alex y Bárbara quieren usar una clave privada para crear un canal seguro usando criptografía AES. Eligen un grupo cíclico finito G de 31 y un generador $\alpha = 3$. Luego, Alex elige el número 8 y Bárbara elige el número 7. Describe que valores se intercambian y que clave privada usaran.

Alex calcula $3^8 \bmod 31 = 20$ y envía 20 a Bárbara
Bárbara calcula $3^7 \bmod 31 = 17$ y envía 17 a Alex
Alice calcula $17^8 \bmod 31 = 18$
Bob calcula $20^7 \bmod 31 = 18$

18 será la clave privada

3) Tiempo de resolución estimado: **15 minutos**
Alex quiere enviar el mensaje 99 a Bárbara cifrándolo usando ElGamal. Alex obtiene el certificado de Bárbara donde consta que su clave pública es (3, 149, 101) y elige el número aleatorio 14. Determina el mensaje cifrado de Alex a Bárbara.

$\alpha^b \in G = 3^{14} \bmod 149 = 69$

$c = m \cdot (\alpha^a)^b \in G = 99 \cdot 101^{14} \bmod 149$

$z = 14 \rightarrow z' = 1110$
bucle 0
$x = 1^2 \bmod 149 = 1$
$z'_0 = 1$
$x = 101 \times 1 \bmod 149 = 101$
bucle 1
$x = 101^2 \bmod 149 = 69$
$z'_1 = 1$
$x = 101 \times 69 \bmod 149 = 115$
bucle 2
$x = 115^2 \bmod 149 = 113$
$z'_2 = 1$

x = 101 x 113 mod 149 = 89

bucle 3

x = 89^2 mod 149 = 24

$z'_3 = 0$

$c = m \cdot (\alpha^a)^b \in G = 99 \cdot 24 \bmod 149 = 141$

Alex envía a Bárbara el mensaje (69, 141)

Algoritmos

- A
  - Elige un número a∈G
  - Computa el valor α^a mod n
  - Envía el resultado a B
- B
  - Elige un número b∈G
  - Computa el valor α^b mod n
  - Envía el resultado a A

- A
  - Recibe α^b mod n
  - Computa $(\alpha^b \bmod n)^a \bmod n = X$
- B
  - Recibe α^a mod n
  - Computa $(\alpha^a \bmod n)^b \bmod n = X$

- Se computa $n = p \cdot q$, donde n será la base del grupo cíclico $\mathbb{Z}_n$
- Se computa la función de Euler $\Phi(n) = (p\text{-}1) \cdot (q\text{-}1)$
- Se elige un entero e menor que $\Phi(n)$ y que sea coprimo de $\Phi(n)$
- Se determina $d = e^{-1} \bmod \Phi(n)$

- El mensaje se cifra con

  $c = m^e \bmod n$
- Se descifra con

  $m = c^d \bmod n$

Exponentiation by squaring (a,z,n) $x = a^z \bmod n$

```
begin
    x = 1;
    z^1 = binary representation of z;
    // starting by the most significant bit
    foreach bit z_i^1 ∈ z^1 do
        x = x^2 mod n;
        // multiply x by a if z_i^1 is equal to one
        if z_i^1 == 1 then
            x = x · a mod n
    return x
```

- Se elige un grupo cíclico finito G de orden n
- Un elemento α de este grupo α∈G
- Un usuario A
  - Elige un número aleatorio a
  - Calcula α^a mod n
  - La clave pública es (α, G, α^a)
- Si B quiere enviar un mensaje $m \in G$ a A, entonces debe
  - Elegir un número aleatorio b y calcular α^b mod n
  - Calcular el mensaje cifrado $c = m \cdot (\alpha^a)^b$ mod n
  - Enviar a A el mensaje (α^b, c)
- A recibe el mensaje cifrado
  - Calcula $x = (\alpha^b)^a$ mod n
  - Calcula el mensaje en claro $m = c \cdot x^{-1}$ mod n