Nombre: **DNI:**

Internet, Seguridad y Distribución de Contenidos Multimedia **ISDCM-MEI**
Curso 2024-25 Q2 **Duración: 15'+1h15'**

Segundo examen parcial **SOLUCION** **2025/05/27**

Preguntas Test (5 puntos). Indicar si las siguientes afirmaciones son ciertas o falsas. Cada respuesta correcta son 0,2 puntos. Cada respuesta incorrecta descuenta **0,2 puntos**.
SE PUEDEN AÑADIR COMENTARIOS PARA JUSTIFICAR LAS RESPUESTAS.

UserA encripta con RSA un mensaje m. El mensaje encriptado resultante c=14 es enviado a UserB.

La clave pública de UserA es:(e, n) = (11, 35). **La clave pública de UserB es:(e, n) = (3, 22)**

Nota: En la firma RSA: $c = m^e \bmod n$; $m = c^d \bmod n$; $d = e^{-1} \bmod \Phi(n)$

1. Podríamos obtener el valor Φ(n) que usa UserA para calcular su clave secreta d porque somos capaces de obtener los números primos p y q que se han usado para calcular n = p * q.

☐ Cierto ☐ Falso

Answer: True. Φ(n)=(p-1)*(q-1)

2. La clave secreta que necesitamos es d = 10.

☐ Cierto ☐ Falso

Answer: False. We need the secret key of UserB. To calculate it, we need Φ(n) = (p-1)*(q-1), being p and q the factors of n (n=p*q). Since in this case n is very small, we may easily deduct that n=22=2*11, so Φ(n) = 1*10=10.
Therefore, the secret key of UserA is $d_A = e_A^{-1} \bmod \Phi_A(n) = 3^{-1} \bmod 10$. We calculate the inverse with the "magic box":

b	d	k
0	10	-
1	3	3
-3	1	

So the result is 10 – 3 = 7. Finally, $d_A = 7 \bmod 10 = 7$.

3. El resultado de la desencriptación de c es m=20.

☐ Cierto ☐ Falso

Answer: True. We apply the formula $m = c^d \bmod n$. Therefore, $m = 14^7 \bmod 22 = 105413504 \bmod 22 = 20$.

4. En el mecanismo ElGamal para encriptación asimétrica, la clave secreta es simplemente un número seleccionado dentro de un rango G dado.

☐ Cierto ☐ Falso

Answer: True.

5. De acuerdo con X.509, la clave pública de una Autoridad de Certificación emitiendo un certificado se debe incluir en dicho certificado.

☐ Cierto ☐ Falso

Answer: False. The Certification Authority Public Key is not included, only its signature.

6. CHACHA20 es el único mecanismo de "stream encryption" soportado en las TLSv1.3 *cipher suites*.

☐ Cierto ☐ Falso

Answer: True.

7. En TLSv1.3, la clave simétrica debe estar siempre encriptada con algoritmos Diffie-Hellman.

☐ Cierto ☐ Falso

Answer: True.

8. QUIC ("*A UDP-Based Multiplexed and Secure Transport*") integra el TLSv1.3 completo.

☐ Cierto ☐ Falso

Answer: False. QUIC provides a security level equivalent to TLSv1.3 and integrated the handshaking process.

9. S/MIME está estandarizado por el IETF. Especifica diferentes mensajes construidos sobre PKCS#7.

☐ Cierto ☐ Falso

Answer: True.

10. La encriptación de un documento con *XML Encryption* incluye un proceso de canonicalización.

☐ Cierto ☐ Falso

Answer: False. It is part of the signature process with *XML Signature*.

11. En XML Signature, tanto en el caso *enveloped* como en el *enveloping*, el elemento `signature` está siempre incluido en el documento XML firmado.

☐ Cierto ☐ Falso

Answer: True.

12. SAML especifica cómo definir JWTs y enviarlos en servicios web basados en REST.

☐ Cierto ☐ Falso

Answer: False. It is defined with XML and it allows to define *security assertions*, which would be equivalent to a JWT, but it does not allow to define them.

13. El cuerpo de una "access token response" en `OAuth 2.0` está siempre representado en XML.

☐ Cierto ☐ Falso

Answer: False. It might be also JSON or plain text.

14. En `OAuth 2.0`, la respuesta a una Authorization Request es un token que se usa para obtener después un Authorization Grant.

☐ Cierto ☐ Falso

Answer: False. The answer to an Authorization Request is an Authorization Grant, which consists in a Credential to obtain an access token.

15. Un "Encrypted JWT" (JWE) contiene un "Protected header", una "Encrypted key" (simétrica), un "Initialization vector", los datos encriptados ("ciphertext") y un "Authentication tag". El vector y el tag son opcionales, mientras que el resto son obligatorios.

☐ Cierto ☐ Falso

Answer: True.

16. OpenID Connect especifica "Claims" para ser usados en JWTs.

☐ Cierto ☐ Falso

Answer: True.

17. En el contexto de control de acceso, el PDP (*Policy Decision Point*), solicitado por el PEP (*Policy Enforcement Point*), utiliza información del PAP (*Policy Administration Point*), que tiene las reglas de privacidad, y el PIP (*Policy Information Point*) para decidir conceder acceso o no.

☐ Cierto ☐ Falso

Answer: True.

18. El "Mandatory Access Control" está basado en el uso de "security labels" (niveles y categorías), mientras que el "Discretionary Access Control" utiliza listas de control de acceso.

☐ Cierto ☐ Falso

Answer: True.

19. XACML es un estándar que permite expresar reglas para control de acceso. Las reglas se pueden agrupar en políticas. El lenguaje permite especificar cómo combinar las reglas dentro de una política.

☐ Cierto ☐ Falso

Answer: True.

20. La exclusividad de los derechos morales se podría negociar.

☐ Cierto ☐ Falso

Answer: False. Moral rights could not be transferred, so "exclusivity" does not apply.

DE LAS PREGUNTAS 21 A 30, SÓLO HAY QUE CONTESTAR UN MÁXIMO DE 5:

21. FHIR (Fast Healthcare Interoperability Resources) es un estándar de HL7 International que especifica recursos usando XML y JSON entre otros estándares.

☐ Cierto ☐ Falso

Answer: True.

22. La encriptación homomórfica es una técnica criptográfica que permite operaciones sobre datos cifrados sin necesidad de descifrarlos.

☐ Cierto ☐ Falso

Answer: True.

23. LoraWan, Zigbee, MQTT o CoAP son protocolos de seguridad para IoT (Internet of Things).

☐ Cierto ☐ Falso

Answer: False. They are IoT protocols.

24. C2PA (Coalition for Content Provenance and Authenticity) define etiquetas para conocer el origen de un contenido.

☐ Cierto ☐ Falso

Answer: True.

25. La seguridad de la información de salud no se mejora con "at-rest encryption", por lo que nunca se utiliza.

☐ Cierto ☐ Falso

Answer: False. It is common use.

26. Se pueden usar dispositivos externos para implementar sistemas "passwordless".

☐ Cierto ☐ Falso

Answer: True.

27. Los ordenadores cuánticos pueden "romper" fácilmente diversos algoritmos de encriptación. Sin embargo, algunos seguirán siendo seguros, como el RSA.

☐ Cierto ☐ Falso

Answer: False.

28. "Random Forest" y "Support Vector Machine" son ejemplos de mecanismos utilizados en "Machine Learning" aplicado a Sistemas de Detección de Intrusos.

☐ Cierto ☐ Falso

Answer: True.

29. Hay técnicas de watermarking "invisible" en el dominio del espacio, pero no en el dominio de la frecuencia.

☐ Cierto ☐ Falso

Answer: False. Both are available.

30. Las "cookies" en el contexto de "web tracking" se almacenan en los servidores, pero no en los navegadores.

☐ Cierto ☐ Falso

Answer: False. The other way around.

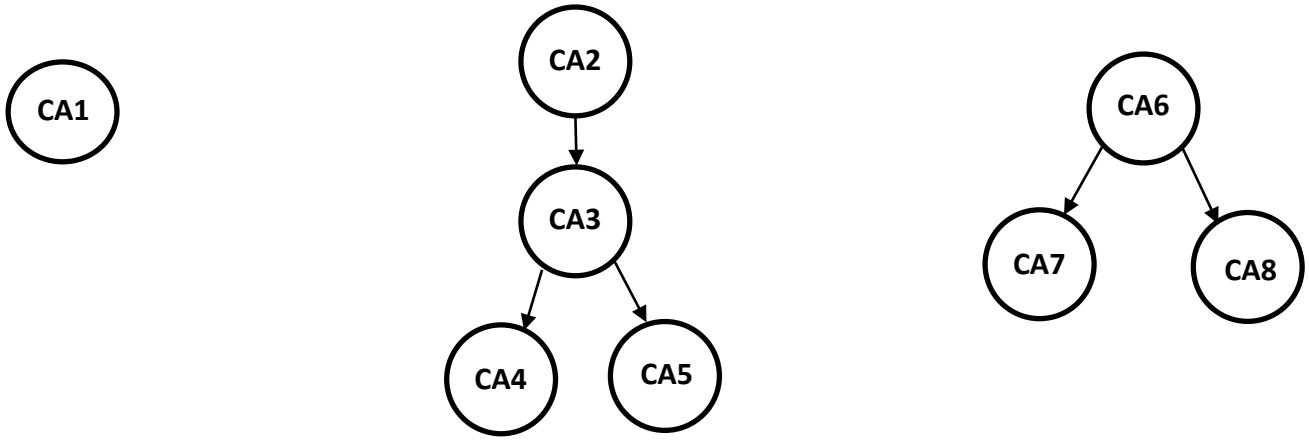
Nombre: **DNI:**

Internet, Seguridad y Distribución de Contenidos Multimedia **ISDCM-MEI**
Curso 2024-25 Q2 **Duración: 15'+1h15'**

Segundo examen parcial **SOLUCION** **2025/05/27**

Problema 1 *(2 puntos)*

Dadas las siguientes CAs organizadas como en las siguientes figuras, donde tenemos estructuras tanto Planas como Jerárquicas:



CA1 emite el certificado C1 para UserA, CA4 emite el C4 para UserB, y CA7 emite el C7 para UserC.

Razonada y brevemente contestar las siguientes preguntas:

a) ¿Cuál o cuáles de los certificados existentes en este sistema incluye(n) la firma de CA3? **b)** Lo mismo para CA7. **c)** ¿Cuál o cuáles de los 3 certificados incluye(n) la firma de UserA? **d)** Si UserA envía contenido encriptado a UserC, ¿qué certificados se han de validar y por quién? **e)** Si UserA recibe el certificado de UserB, ¿lo aceptará? En caso afirmativo, ¿qué usuario podría enviar información encriptada a qué usuario? **f)** UserB no podría envíar contenido encriptado a UserC porque el certificado intercambiado no sería aceptado. ¿Qué Autoridad(es) de Certificación podría(n) resolver el problema y cómo?

a) CA3 only signs the certificates it issues. In this case, CA4 and CA5.

b) C7.

c) Users never sign their certificates.

d) UserA validates C7 (UserC's certificate issued by CA4) and CA7's certificates. We could also consider the validation of CA6's certificate.

e) No, because their CAs are independent and do not trust each other; i.e., it is rejected because both users are in independent trust hierarchies.

f) The CAs issuing the certificates of both users (CA4 and CA7) could cross-certify between them, or could connect to the same bridge-CA. In addition, the upper CAs could do the same, in any combination. For example, CA2 and CA6 (the most probable case, since they are the root CAs), or CA3 and CA6, to say a few.

Problema 2 *(1,5 puntos)*

Tenemos la siguiente parte de una instancia de documento XML parcialmente protegido:

```
<HealthRecord xmlns='http://example.org/healthrecord'>
      <Name>Pep Roca</Name>
      <Age>60</Age>
      <BloodTest>
            <Cholesterol>200</Cholesterol>
            <EncryptedData
            Type='http://www.w3.org/2001/04/xmlenc#Element'
            xmlns='http://www.w3.org/2001/04/xmlenc#'>
                  <CipherData>
                        <CipherReference
                        uri='http://example.org/healthrecord/blood1'
                        />
                  </CipherData>
            </EncryptedData>
      </BloodTest>
</HealthRecord>
```

Contestar razonada y brevemente las siguientes preguntas:

a) ¿Qué elementos XML contenía el elemento `BloodTest` antes de ser encriptado? **b)** Modificar el elemento `HealthRecord` encriptando también el valor del nivel de colesterol de `Pep Roca`. Dar un valor al elemento `CipherValue` que se incluya, así como al atributo `Type`. **c)** Ahora queremos encriptar todo el documento XML. ¿Cómo quedaría?

```
a) "Cholesterol" and one encrypted element.

b)
<HealthRecord>
   <Name>Pep Roca</Name>
   <Age>60</Age>
   <BloodTest>
      <Cholesterol>
          <EncryptedData
           Type='http://www.w3.org/2001/04/xmlenc#Content'
           xmlns='http://www.w3.org/2001/04/xmlenc#'>
             <CipherData>
                  <CipherValue>CBBSDEESA</CipherValue>
             </CipherData>
         </EncryptedData>
      </Cholesterol>
      <EncryptedData…</EncryptedData>
    </BloodTest>
</HealthRecord>

c)
<EncryptedData
   Type='http://www.w3.org/2001/04/xmlenc#Element'
   xmlns='http://www.w3.org/2001/04/xmlenc#'>
        <CipherData>
             <CipherValue>ABCSBDEFESA</CipherValue>
        </CipherData>
</EncryptedData>
```

Problema 3 (*1,5 puntos*)

Disponemos de estos tres fragmentos de reglas o solicitudes de control de acceso expresadas en lenguaje XACML v3.0.

Fragmento 1

```
<Rule RuleId="urn:oasis:names:tc:xacml:3.0:RuleSAM" Effect="Permit">
…
<Match MatchId="urn:oasis:names:tc:xacml:1.0:function:string-equal">
  <AttributeValue DataType="http://www.w3.org/2001/XMLSchema#string">
       View
  </AttributeValue>
  <AttributeDesignator MustBePresent="false"
     Category="urn:oasis:names:tc:xacml:3.0:attribute-category:action"
     AttributeId="urn:oasis:names:tc:xacml:1.0:action:action-id"
     DataType="http://www.w3.org/2001/XMLSchema#string"/>
</Match>

<Match MatchId="urn:oasis:names:tc:xacml:1.0: function:date-less-than-or-equal">
  <AttributeValue DataType="http://www.w3.org/2001/XMLSchema#date">
       2025-12-31
  </AttributeValue>
  <AttributeDesignator MustBePresent="false"
     Category="urn:oasis:names:tc:xacml:3.0:date"
     AttributeId="accesDate"
     DataType="http://www.w3.org/2001/XMLSchema#date"/>
</Match>
   …
</Rule>
```

Fragmento 2

```
<Rule RuleId="urn:oasis:names:tc:xacml:3.0:RuleSAM" Effect="Permit">
   …
   <Match MatchId="urn:oasis:names:tc:xacml:1.0:function:regexp-string-match">
     <AttributeValue DataType="http://www.w3.org/2001/XMLSchema#string">
          urn:mvideo:videoA.mp4
     </AttributeValue>
     <AttributeDesignator MustBePresent="false"
        Category="urn:oasis:names:tc:xacml:3.0:attribute-category:resource"
        AttributeId="urn:oasis:names:tc:xacml:1.0:resource:resource-id"
        DataType="http://www.w3.org/2001/XMLSchema#string"/>
  </Match>
…
</Rule>
```

Fragmento 3

```
…
<Attributes Category="urn:oasis:names:tc:xacml:3.0:attribute-category:action">
     <Attribute AttributeId="urn:oasis:names:tc:xacml:1.0:action:action-id"
         IncludeInResult="true">
         <AttributeValue DataType="http://www.w3.org/2001/XMLSchema#string">
             TO COMPLETE
         </AttributeValue>
     </Attribute>
</Attributes>
…
<Attributes Category="urn:oasis:names:tc:xacml:3.0:date">
     <Attribute AttributeId="accessDate" IncludeInResult="true">
         <AttributeValue DataType="http://www.w3.org/2001/XMLSchema#date">
             TO COMPLETE
         </AttributeValue>
     </Attribute>
</Attributes>
…
```

Contestar razonada y brevemente las siguientes preguntas:

1) El Fragmento 1, ¿qué acción y condición define?

View is the action, and date is the condition (<=25/12/31).

2) El Fragmento 2 es también parte de una regla. **a)** ¿Cuál es el "efecto" de la regla? **b)** ¿Qué define el `Match`? **c)** Si combinamos los fragmentos 1 y 2, dar los valores de los campos de un XACML Request para poder autorizar la visualización de un vídeo en una fecha concreta. **d)** ¿Qué atributo faltaría para hacer completa la regla?

a) Allow.

b) A resource.

c) "View" for the Action, "2025-05-27" (for example) for the date and "urn:mvideo:videoA.mp4" for the resource.

d) Who is authorized by the rule: the user.

3) Completar el Fragmento 3 (XACML Request) con valores que hagan que se cumpla la regla del fragmento 1.

"View" and "2025-05-27", as before.