# IC/ASC - 2022

Cuarto parcial

14/11/2022

Facultad de Informática

**NOMBRE y APELLIDO:..... Legajo (o DNI): …….**

**Para aprobar y promocionar se requieren obtener 6 y 7 puntos respectivamente.**

**1. (1 punto)** Clasificar las siguientes afirmaciones si se refieren a una vulnerabilidad, amenaza o ataque:

- Un empleado deja un papel pegado al monitor con una contraseña. Vulnerabilidad
- Se realiza un acceso no autorizado al sistema de información. Ataque
- Un empleado no actualiza la contraseña inicial asignada por el administrador del sistema. Vulnerabilidad

**2. (1 punto)** Elegir la opción correcta que completa las palabras faltantes de la frase: "Queremos enviar un documento por una red insegura de manera que sea legible sólo por el receptor del mismo. El documento será cifrado con la clave (1) del (2)".

- ☐ (1) privada (2) receptor
- ☒ (1) pública (2) receptor
- ☐ (1) privada (2) emisor
- ☐ (1) pública (2) emisor

**3. (2 puntos)** Marcar cada opción correcta:

- ☐ La desventaja de la criptografía simétrica es la alta cantidad de cómputo que requiere (en comparación con la criptografía asimétrica).
- ☒ Una de las ventajas de la criptografía asimétrica es que no hace falta intercambiar una clave secreta entre el emisor y el receptor.
- ☒ Una de las ventajas de la criptografía asimétrica es que se administran menos claves.
- ☐ En la criptografía asimétrica, para asegurar la confidencialidad, el emisor debe cifrar el mensaje con su clave privada y envíar el texto cifrado.
- ☒ En la criptografía asimétrica, para asegurar la autenticidad, el emisor debe cifrar el mensaje con su clave privada y envíar el texto cifrado.

**4. (1 punto)** Marcar cada opción correcta.

La firma digital, que utiliza cifrado de código hash y clave pública certificada, garantiza:

- ☒ No repudio
- ☐ Disponibilidad
- ☐ Confidencialidad
- ☒ Integridad
- ☒ Autenticidad

**5. (1 punto)** Marcar la opción correcta en relación a los enunciados sobre el código de autenticación de mensajes:

- ☐ El emisor transfiere únicamente el mensaje cifrado con su clave privada.
- ☐ El emisor transfiere únicamente el código hash del mensaje.
- ☐ El emisor transfiere únicamente el mensaje cifrado con la clave pública del receptor.
- ☐ El emisor transfiere únicamente el código hash calculado a partir de la unión del mensaje y un código conocido sólo por el emisor y receptor.
- ☒ Ninguna de las opciones anteriores es correcta.

**6. (1 punto)** Elegir la opción correcta que completa las palabras faltantes de la frase: **"**Para soportar el protocolo de transferencia de páginas web denominado (1), es necesario instalar en el servidor (2) digital, que emitió una (3)."

- ☐ (1) HTTPS - (2) una firma - (3) autoridad certificante
- ☒ (1) HTTPS - (2) un certificado - (3) autoridad certificante
- ☐ (1) HTTP - (2) TLS - (3) institución gubernamental
- ☐ (1) HTTPS - (2) un certificado - (3) institución gubernamental
- ☐ (1) TLS - (2) un certificado - (3) autoridad certificante
- ☐ (1) HTTP - (2) un certificado - (3) autoridad certificante

**7. (1 punto)** Escriba el comando (y opciones) de GPG que genera un par de claves pública-privada: gpg --full-generate-key

**8. (1 punto)** Marcar la opción correcta. El comando "gpg --armor --export *apellido* | curl -T - https://keys.openpgp.org" sirve para:

- ☐ subir la clave privada a un servidor de claves de GPG.
- ☒ subir la clave pública a un servidor de claves de GPG.
- ☐ subir las claves pública y privada a un servidor de claves de GPG.

**9. (1 punto)** Marcar cada opción correcta. En la firma digital con GPG, para verificar la firma es necesario:

- ☐ disponer del código hash del firmante.
- ☐ disponer de la clave privada del firmante.
- ☒ disponer de la clave pública del firmante.
- ☐ disponer de la clave privada del receptor.
- ☐ disponer de la clave pública del receptor.
- ☒ que GPG genere el código hash del documento para compararlo con el código hash (del documento) que viene cifrado y debe descifrar.