1) Un criptosistema de clave secreta es aquel en el que...

a) Emisor y receptor conocen y comparten una misma clave.

b) Emisor y receptor utilizan una clave para cifrar (clave secreta) y otra clave para descifrar (clave pública).

c) Emisor y receptor utilizan una clave para cifrar (clave pública) y otra clave para descifrar (clave secreta).

d) Ninguna de las respuestas anteriores es correcta.

---

2) ¿Cuál de las siguientes afirmaciones es cierta?

a) MD5 es un algoritmo hash.

b) RSA es un algoritmo de cifrado asimétrico.

c) AES es un algoritmo de cifrado simétrico.

d) Todas las respuestas son correctas.

---

3) ¿Cuál de las siguientes afirmaciones sobre el cifrado de clave asimétrica para enviar mensajes confidenciales es cierta?

a) La parte que envía el mensaje cifra el mensaje con su propia clave privada.

b) La parte que envía el mensaje cifra el mensaje con su propia clave pública.

c) La parte que recibe el mensaje descifra el mensaje con su propia clave privada.

d) La parte que recibe el mensaje descifra el mensaje con su propia clave pública.

---

4) La firma electrónica...

a) Se basa en los sistemas de clave simétrica.

b) Se basa en los sistemas de clave asimétrica.

c) Tiene su origen en los sistemas híbridos como PGP.

d) Ninguna de las respuestas es correcta.

---

5) ¿En qué cosiste la encriptación?

a) En cerrar los ordenadores en zonas subterráneas de seguridad o criptas.

b) En realizar copias de seguridad para luego guardarlas en cajas de seguridad.

c) En cifrar la información para que no tenga sentido ante un usuario no autorizado.

d) En utilizar siempre mensajes de texto en las comunicaciones de red.

---

6) ¿Para qué se utiliza el algoritmo hash?

a) Para proteger las contraseñas.

b) Para generar la firma digital.

c) Para garantizar la integridad de la información.

d) Todas las respuestas son correctas.

---

7) ¿Cuál de las siguientes opciones realizará Andrés para comprobar que un mensaje procede de Paula si se utiliza cifrado de clave asimétrica?

a) Andrés utilizará la clave privada de Paula para descifrar el mensaje.

b) Andrés utilizará su clave privada para descifrar el mensaje.

c) Andrés utilizará la clave pública de Paula para descifrar el mensaje.

d) Andrés utilizará su clave pública para descifrar el mensaje.

8) ¿Cuál de las siguientes opciones no es una ventaja de los sistemas de cifrado simétrico?

a) Son más rápidos que los asimétricos.
b) Resultan apropiados para cifrar grandes volúmenes de datos.
c) Utilizan un menor número de claves que los asimétricos.
d) Requieren claves de menor tamaño que los asimétricos para garantizar la seguridad.

---

9) ¿Cuál de las siguientes afirmaciones es cierta?

a) RSA y DSA son algoritmos de cifrado simétrico.
b) DES y AES son algoritmos de cifrado asimétrico.
c) Los algoritmos de cifrado simétrico son más rápidos que los de cifrado asimétrico.
d) Todas las respuestas anteriores son correctas.

---

10) ¿Cuál de los siguientes se considera un criptosistema híbrido?

a) RSA.
b) PGP.
c) IDEA.
d) AES.

1) ¿Cuál de las siguientes opciones es cierta?

a) Si un desconocido consigue la clave privada de Juan, podrá enviar mensajes en nombre de Juan.

b) Si un desconocido consigue la clave pública de Juan, podrá enviar mensajes en nombre de Juan.

c) Si un desconocido consigue la clave pública de Juan, podrá descifrar todos los mensajes que le lleguen a Juan.

d) Si un desconocido consigue la clave privada de Juan, podrá enviarle mensajes cifrados.

---

2) ¿Cuál de las siguientes afirmaciones es falsa?

a) RSA es un algoritmo hash.

b) GnuPGP es una herramienta que utiliza algoritmos no patentados.

c) RC5 es un algoritmo de cifrado asimétrico.

d) DES es un algoritmo de cifrado simétrico.

---

3) Si Andrés quiere descifrar un mensaje que le ha enviado Paula mediante el cifrado de clave asimétrica...

a) Utilizará la clave privada de Paula para descifrar el mensaje.

b) Utilizará su clave privada para descifrar el mensaje.

c) Utilizará la clave pública de Paula para descifrar el mensaje.

d) Utilizará su clave pública para descifrar el mensaje.

---

4) ¿Cómo se denomina el arte de escribir con clave secreta o de un modo enigmático?

a) Criptografía.

b) Criptoanálisis.

c) Criptosistema.

d) Esteganografía.

---

5) ¿Cuál de las siguientes afirmaciones es cierta?

a) Los sistemas híbridos son más rápidos que los sistemas simétricos.

b) Los sistemas híbridos permiten el intercambio de claves en entornos no seguros, al contrario que los asimétricos.

c) Las dos afirmaciones anteriores son ciertas.

d) Ninguna de las afirmaciones anteriores es cierta.

---

6) ¿Cuál de las siguientes opciones es una propiedad de la función hash?

a) Un mensaje largo producirá una huella más larga que un mensaje corto porque la cantidad de caracteres a codificar será mayor.

b) La huella producida es completamente distinta si se cambia un solo bit.

c) No es posible encontrar dos entradas que den lugar al mismo valor hash.

d) Resulta computacionalmente imposible obtener el mensaje original a partir del resultado de aplicar una función hash.

7) ¿Cuál de las siguientes afirmaciones es cierta?

a) Los sistemas de cifrado asimétrico requieren claves de mayor tamaño que los simétricos para garantizar la seguridad.
b) El intercambio de la clave pública no es un problema en los sistemas de cifrado asimétrico.
c) Los sistemas de cifrado simétrico son más rápidos que los de cifrado asimétrico.
d) Todas las respuestas son correctas.

---

8) Los criptosistemas de cifrado simétrico...

a) También se denominan de clave pública.
b) Utilizan un algoritmo de cifrado que realiza varias sustituciones y transformaciones del texto nativo.
c) Utilizan un sistema de dos claves, una privada y otra pública.
d) Todas las respuestas son correctas.

---

10) Si Marta quiere enviar a Pablo, utilizando cifrado de clave asimétrica, un mensaje de manera que Pablo sepa que ese mensaje es de ella...

a) Marta utilizará la clave privada de Pablo para cifrar el mensaje.
b) Marta utilizará su clave privada para cifrar el mensaje.
c) Marta utilizará la clave pública de Pablo para cifrar el mensaje.
d) Marta utilizará su clave pública para cifrar el mensaje.

1) ¿Cuál de las siguientes afirmaciones es cierta?

a) Los sistemas de cifrado asimétrico requieren claves de mayor tamaño que los simétricos para garantizar la seguridad.
b) El intercambio de la clave pública no es un problema en los sistemas de cifrado asimétrico.
c) Los sistemas de cifrado simétrico son más rápidos que los de cifrado asimétrico.
d) Todas las respuestas son correctas.

---

2) ¿Qué es una clave de un sistema criptográfico?

a) Un conjunto de signos o símbolos del mensaje original a los que se les cambia la posición.
b) Una herramienta necesaria para enviar un archivo por Internet.
c) Un conjunto de signos utilizados para transmitir un mensaje privado cuyo contenido se quiere ocultar.
d) Ninguna de las respuestas anteriores es correcta.

---

3) Las claves de los certificados del DNI electrónico...

a) Utilizan el sistema de cifrado simétrico.
b) Utilizan el sistema de cifrado asimétrico.
c) No utilizan ninguno de estos dos métodos.
d) Pueden utilizar ambos métodos por igual.

---

5) ¿Cuál de las siguientes opciones es cierta?

a) Si un desconocido consigue la clave privada de Juan, podrá enviar mensajes en nombre de Juan.
b) Si un desconocido consigue la clave pública de Juan, podrá enviar mensajes en nombre de Juan.
c) Si un desconocido consigue la clave pública de Juan, podrá descifrar todos los mensajes que le lleguen a Juan.
d) Si un desconocido consigue la clave privada de Juan, podrá enviarle mensajes cifrados.

---

7) PGP es un algoritmo...

a) Con características únicamente de la criptografía simétrica.
b) Con características únicamente de la criptografía asimétrica.
c) Al que se le puede considerar como un criptosistema híbrido.
d) Ninguna de las respuestas anteriores es cierta.

---

9) Un criptosistema de clave asimétrica es aquel donde...

a) Emisor y receptor conocen y comparten una misma clave.
b) El emisor utiliza una clave para cifrar (clave privada) y el receptor utiliza una clave diferente para descifrar (clave pública).
c) El emisor utiliza una clave para cifrar (clave pública) y el receptor utiliza una clave diferente para descifrar (clave privada).
d) Se utiliza una clave para cifrar (clave secreta) y se descifra con otra clave diferente.