

127

Sistemas de seguridad en la empresa

Test módulo 3

- 1.- Elegir las opciones que no garantizan los sistemas de cifrado simétrico
 - a. Confidencialidad
 - b. Autenticidad de origen
 - c. Integridad
 - d. No repudio
- 2.- En los sistemas de cifrado asimétrico si se compromete la clave pública se compromete toda la comunicación
 - a. Verdadero
 - b. Falso
- 3.- Cual de los cifrados no se considera un sistema de cifrado clásico
 - a. Cifrados por transposición (o permutación).
 - b. Cifrados por sustitución.
 - c. Cifrado utilizando claves secretas de gran longitud.
 - d. Cifrado por sistema de sustitución polialfabeto.

Curso ciberseguridad por José Manuel Aroca Fernández

14-Nov-21

127

128

Sistemas de seguridad en la empresa

Test módulo 3

- 4.- Identifica el sistema que usa los pasos del cifrado descrito por los pasos siguientes y ordénalos
 - a) Si el usuario B quiere comunicarse con A usa la clave pública de éste.
 - b) Cuando A recibe un mensaje cifrado de B lo descifra usando su clave privada.
 - c) Cada usuario deposita su clave pública en un lugar accesible.
 - d) Cada usuario genera un par de claves: la pública y la privada.
- 5.- Identifica el sistema que usa los pasos del cifrado descrito por los pasos siguientes y ordénalos
 - a) Los usuarios comparten las mismas claves.
 - b) Si el usuario B quiere comunicarse con A usa la clave privada compartida.
 - c) Cuando A recibe un mensaje cifrado de B lo descifra usando su clave privada.
- 6.- ¿Cual de las siguientes afirmaciones es falsa en los sistemas de cifrado asimétrico?
 1. Si un usuario (emisor) quiere enviar un mensaje secreto a otro (receptor), debe cifrarlo utilizando su clave pública.
 2. El mensaje tan solo puede descifrarse utilizando la clave privada del receptor, con lo que se garantiza la confidencialidad del mismo.
 3. La clave pública del receptor no sirve para descifrar el mensaje, y por tanto tan solo el receptor (que es el único que conoce su propia clave privada), puede descifrarlo.

Curso ciberseguridad por José Manuel Aroca Fernández

14-Nov-21

128

129

Sistemas de seguridad en la empresa

Test módulo 3

7.- Las criptomonedas, en nuestro caso los Bitcoins se obtienen mediante ataques por fuerza bruta

1. Verdadero
2. Falso

8.- ¿Qué es un bitcoin?

1. Es una moneda virtual que cotiza en mercados alternativos y garantiza altas rentabilidades
2. Es a la vez un protocolo, una red de pagos y una moneda
3. Es una criptomoneda basada en una red anónima que permite hacer pagos sin pagar a Hacienda

9.- ¿Qué es blockchain?

1. Es una tecnología que permite almacenamiento de datos sin que nadie pueda manipularlo
2. Es un sistema alternativo de transferencia de fondos
3. Es un Sistema complejo de liquidación de valores

Curso ciberseguridad por José Manuel Aroca Fernández

14-Nov-21

129

130

Sistemas de seguridad en la empresa

Test módulo 3

10.- ¿Qué retardo llevan las transacciones con bitcoin?

1. Ninguno, es inmediato
2. Media hora
3. 10 minutos
4. 20 minutos

11.- ¿Qué hay que hacer para ser un minero de bitcoin?

1. Es necesario especializarse accediendo a centros de datos desarrollados
2. Basta con sacar un certificado digital avanzado
3. Cualquiera puede serlo si utiliza un software y hardware especializado

12.- ¿Cuál de los elementos siguientes no es un elemento básico del Blockchain?

1. Nodo
2. Protocolo o estándares
3. Red entre pares P2P
4. Minero

Curso ciberseguridad por José Manuel Aroca Fernández

14-Nov-21

130