Apellido, Nombre: Documento: Fecha:

1 - ¿ Para que se utiliza la firma digital ?
A - Generar datos aleatorios
B - Garantizar la confidencialidad de datos
C - Garantizar la autenticidad de datos
D - Ninguna de estas opciones

2 - ¿ Cuál de los siguientes algoritmos es denominado AES ?
A - Serpent
B - Rijndael
C - IDEA
D - DES

3 - ¿ Que condiciona el libre uso de los algoritmos ?
A - Ninguna de estas opciones
B - Que sean públicos
C - Que tengan patentes en vigencia
D - Que sean privados

4 - ¿ Cual de los siguientes elementos no corresponde a una funcion de negocio de SAMM ?
A - Gobierno
B - Implementación
C - Verificación
D - Diseño
E - Construcción

5 - ¿ Cuál de los siguientes elementos NO corresponde a una característica positiva de los sistemas criptográficos simétricos ?
A - Robustez
B - Velocidad de cifrado
C - Longitud del mensaje limitada por la implementación
D - Sencillez de implementación

6 - ¿ Cual de los siguientes NO es un modo de cifrado de bloques ?
A - CBC - Cipher Block Chaining
B - OFB - Output Feedback
C - CFB - Cipher Feedback
D - Ninguna de las opciones

7 - ¿ Cuál de las siguientes NO es una propiedad de la firma digital ?
A - Va ligada indisolublemente al mensaje
B - Se genera en base a la clave pública del destinatario
C - Sólo puede ser generada por su legítimo titular
D - Es públicamente verificable

8 - ¿ Qué significa el acrónimo CMM ?
A - Capacity Model Metrics
B - Capability Maturity Model
C - Capability Model and Metrics
D - Capacity Measure Model

9 - ¿ Que norma define la metodología de SCRUM ?
A - Ninguna de estas opciones
B - ISO 25000
C - ISO/IEC 9126
D - ISO/IEC 14598

10 - Determine el mensaje original para el siguiente cifrado obtenido mediante el cifrado de XOR solamente.
Valor cifrado: 101110110010
Contraseña : 011100110110
Se conoce la existencia del los siguientes valores binarios 100111000011 y 110011110011.
A - 101010100011
B - 110010000100
C - 001110110110
D - 111100111010

11 - ¿ A que se denomina "Padding" ?
A - Al método para autenticar mensajes con algoritmos asimétricos
B - Al método para completar el inicio de un bloque de datos
C - Al método que permite generar una distorsión entre los distintos bloques
D - Al método para completar el final de un bloque de datos

Documento: Fecha:

12 - ¿ Cuál de los siguientes datos NO está contenido en los campos de un certificado X509 ?
A - Número de serie
B - Nombre del sujeto
C - Clave privada del sujeto
D - Clave pública del sujeto

13 - ¿ Cuál de los siguientes puntos no es de interés para el manejo de sesiones de estado ?
A - Seguridad de transporte
B - Ataques de autenticación de sesión
C - Páginas y credenciales en formularios
D - Entropía de credencial de sesión

14 - ¿ Cual de estos elementos no corresponde a la lista de requerimientos verificacion de ASVS2014 ?
A - Cryptography at Rest
B - Authentication
C - Data Protection
D - Communications
E - Mobile
F - Performance

15 - Indique cual es la definición correcta de j según la siguiente representación de un sistema criptográfico: Dj (Ej (m)) = m
A - Representa el conjunto de transformaciones de cifrado
B - Representa el conjunto de claves que se pueden emplear
C - Representa el conjunto de todos los mensajes sin cifrar
D - Representa el conjunto de todos los posibles mensajes cifrados

16 - ¿ Cual de los siguientes elementos NO se corresponde con una propiedad de la Calidad en Uso ?
A - Productividad
B - Seguridad
C - Satisfacción
D - Eficacia
E - Ninguna de las opciones

17 - ¿ Que establece el marco legal para el uso de la Firma Digital en la República Argentina ?
A - El Pacto de San Jose de Costa Rica
B - La ley 25.506
C - La ley 24.449
D - La Constitución Nacional

18 - ¿ Que caracteristica de calidad Interna/Externa NO esta contemplada en SQuaRE ?
A - Portabilidad
B - Mantenibilidad
C - Ninguna de estas opciones
D - Fiabilidad

19 - ¿ A que tipo de algoritmo corresponde el cifrado del Cesar ?
A - Cifrado por transposición de grupos
B - Cifrado por sustitución
C - Cifrado Asimétrico
D - Cifrado de simétrico de flujo

20 - ¿ Cuál de los siguientes puntos NO es un objetivo de la administración de usuarios y privilegios ?
A - Los usuarios no pueden acceder o utilizar funcionalidades administrativas
B - Las funciones de nivel de administrador están segregadas apropiadamente de la actividad del usuario
C - Los usuarios transmiten información de manera cifrada y confidencial
D - Proveer la necesaria auditoria y trazabilidad de funcionalidad administrativa

21 - ¿ Cual de estos elementos corresponde a la escala con que se representan los niveles de madurez de SAMM ?
A - A,B,C
B - Bajo, Medio, Alto
C - 1, 2, 3, 4, 5, 6, 7, 8, 9, 10
D - 0, 1, 2, 3

...Cesar: "od uhvsxhvwd fruuhfwd frqwlhqh od sdodeud ixhrs" según indica el siguiente mensaje generado mediante

Apellido, Nombre:

Documento: Fecha:

22 - ¿ Sobre qué tecnología están desarrollados los Web Services ?
- A - XML/SOAP
- B - HTTPS
- C - AES
- D - HTML

23 - Indique a qué corresponde la siguiente definición: "Se define como una función o método para generar un valor que represente de manera casi unívoca a un dato. "
- A - Función de encriptación de datos
- B - Función de descifrado de datos
- C - Función hash
- D - Función de firma digital

24 - Indique cual es el ordene creciente en base al nivel de seguridad de las siguientes técnicas de autenticación de usuarios
- A - Básica y segura, Basada en formas, Integrada, Fuerte, Basada en certificado
- B - Basada en formas, Básica y segura, Integrada, Fuerte, Basada en certificado
- C - Básica y segura, Integrada, Basada en formas, Basada en certificado, Fuerte
- D - Básica y segura, Basada en formas, Integrada, Basada en certificado, Fuerte
- E - Basada en formas, Básica y segura, Integrada, Basada en certificado, Fuerte

25 - ¿ Cual de estos elementos corresponde a un nivel que no define requerimientos detallados de verificación en ASVS ?
- A - Advanced
- B - Cursory
- C - Opportunistic
- D - Standard

26 - ¿ Qué cantidad de PAs están definidos para el SSE-CMM ?
- A - 24
- B - 16
- C - 18
- D - 22

27 - ¿ Que modelo de autorización utiliza un sistema UNIX/Linux convencional para manejar sus archivos ?
- A - Mandatory Access Control (MAC)
- B - Discretionary Access Control (DAC)
- C - Role Based Access Control (RBAC)
- D - Ninguna de estas opciones

28 - Marque la respuesta correcta según indica el siguiente mensaje generado mediante el cifrado del Cesar: "od uhvsxhvwd fruuhfwd frqwlhqh od sdodeud ixhjr"
- A - Los fideos tienen salsa
- B - Hay estrellas en el cielo
- C - La torre es demasiado alta
- D - El fuego se apagara pronto

29 - ¿ Qué mecanismo adiciona criptografía al proceso de hash con el fin de incorporar autenticación a la seguridad del mismo ?
- A - MD5
- B - MAC
- C - AES
- D - Ninguna de estas opciones

30 - ¿ Cuál de los siguientes algoritmos se basa en la dificultad para factorizar grandes números ?
- A - Ninguna de estas opciones
- B - RSA
- C - AES
- D - ElGamal