Seguridad y calidad en aplicaciones web – Segundo Parcial

1. ¿Para qué se utiliza la firma digital? **C. Garantizar la autenticidad de datos**
2. ¿Cuál de los siguientes algoritmos es denominado AES? **B. Rijndael**
3. ¿Que condiciona el libre uso de los algoritmos? **C. Que tengan patentes en vigencia**
4. ¿Cuál de los siguientes elementos no corresponde a una función de negocio de SAMM? **D. Diseño**
5. ¿Cuál de los siguientes elementos NO corresponde a una característica positiva de los sistemas criptográficos simétricos? **C. Longitud del mensaje limitada por la implementación**
6. ¿Cuál de los siguientes NO es un modo de cifrado de bloques? **D. Ninguna de las opciones.**
7. ¿Cuál de las siguientes NO es una propiedad de la firma digital? **B. Se genera en base a la clave publica del destinatario.**
8. ¿Qué significa el acrónimo CMM? **A. Capability Maturity Model**
9. ¿Qué norma define la metodología de SCRUM? **A. Ninguna de estas opciones**
10. Determine el mensaje original para el siguiente cifrado obtenido mediante el cifrado XOR solamente: **B.110010000100**
11. ¿A qué se denomina "Padding"? **D. Al método para completar el final de un bloque de datos**
12. ¿Cuál de los siguientes datos NO está contenido en los campos de un certificado X509? **C. Clave privada del sujeto**
13. ¿Cuál de los siguientes puntos no es de interés para el manejo de sesiones de estado? **D. Entropia de credencial de sesión**
14. ¿Cuál de estos elementos NO corresponde a la lista de requerimientos verificación de ASVS 2014? **F. Performance**
15. Indique cuál es la definición correcta de j según la siguiente representación de un sistema criptográfico: **A. Representa el conjunto de transformaciones de cifrado.**
16. ¿Cuál de los siguientes elementos NO se corresponde con una propiedad de la Calidad en SQaRE? **E. Ninguna de las opciones**
17. ¿Qué establece el marco legal para el uso de la Firma Digital en la República Argentina? **B. La ley 25.506**
18. ¿Qué característica de calidad Interna/Externa NO está contemplada en SQaRE? **C. Ninguna de estas opciones**
19. ¿A qué tipo de algoritmo corresponde el cifrado del Cesar? **B. Cifrado por sustitución**
20. ¿Cuál de los siguientes puntos NO es un objetivo de la administración de usuarios y privilegios? **C. Los usuarios transmiten información de manera cifrada y confidencial**
21. ¿Cuál de estos elementos corresponde a la escala con que se representan los niveles de madurez de SAMM? **D. 0, 1, 2, 3**
22. ¿Sobre qué tecnología están desarrollados los Web Services? **A. XML/SOAP**
23. Indique a qué corresponde la siguiente definición: "Se define como una función o método para generar un valor que represente de manera casi única a un dato. **C. Función hash**
24. Indique cuál es el orden creciente en base al nivel de seguridad de las siguientes técnicas de autenticación de usuarios: **D. Básica y segura, Basada en formas, Integrada, Fuerte, Basada en certificado**
25. ¿Cuál de estos elementos corresponde a un nivel que no define requerimientos detallados de verificación en ASVS? **B. Cursory**
26. ¿Qué estándar de PAS están definidos para el SSE-CMM? **D. 22**
27. ¿Qué modelo de autorización utiliza un sistema UNIX/Linux convencional para manejar sus archivos?
    - Respuesta seleccionada: **B. Discretionary Access Control (DAC)**
28. Marque la respuesta correcta según indica el siguiente mensaje generado mediante el cifrado del Cesar: "od uhwxswhvw fruuhfw frqwhqido gh soddo idxjr" **D. El fuego se apagará pronto.**
29. ¿Qué mecanismo adiciona criptografía al proceso de hash con el fin de incorporar autenticación a la seguridad del mismo? **D. MAC**
30. ¿Cuál de los siguientes algoritmos se basa en la dificultad para factorizar grandes números? **B. RSA**

Seguridad y calidad en aplicaciones web – Recuperatorio 2do parcial

1) ¿Qué estándar se ha definido para la seguridad específica de Web Services? **D. WSS**
2) ¿Cuál de los siguientes puntos NO es un objetivo de la administración de usuarios y privilegios? **C. Los usuarios transmiten información de manera cifrada y confidencial.**
3) Indique cual es el orden creciente en base al nivel de seguridad de las siguientes técnicas de autenticación de usuarios. **C. Basica y segura, Basada en formas, Integrada, Basada en certificado, Fuerte.**
4) Dada la clave pública (p, y, n) y la clave privada (p, x, n). Indique a que algoritmo corresponden las siguientes definiciones de cifrado: A=p^k (mod n) - B=y^k m (mod n) **A. ElGamal**
5) ¿Qué mecanismo adiciona criptografía al proceso de hash con el fin de incorporar autenticación a la seguridad del mismo? **A. MAC**
6) ¿Cuál es el significado de SSL? **A. Secure Sockets Layer**
7) ¿Cuál de los siguientes elementos NO se corresponde con una propiedad de la Calidad en Uso? **B-Ninguna de las opciones.**
8) Indique cual es la definición correcta de j según la siguiente representación de un sistema criptográfico: Dj (Ej (m)) = m. **D. Representa el conjunto de claves que se pueden emplear.**
9) Indique a que corresponde la siguiente definición: “Se define como una función o método para generar un valor que represente de manera casi unívoca a un dato.” **C. Función hash.**
10) ¿Cuál de estos elementos no corresponde a la lista de requerimientos verificación de ASVS2014? **E. Performance.**
11) ¿Cuál es la diferencia entre SSE-CMM y ASVS? Desarrolle los detalles y casos de aplicación de cada uno de estos elementos en su respuesta.
12) Enumere, defina y relacione las etapas del proceso de gestión de la “Calidad Total” y su vínculo con el modelo SCRUM.