1. ¿Para que se utiliza la firma digital?
2. Generar datos aleatorios
3. Garantizar la confidencialidad de datos
4. Garantizar la autenticidad de datos
5. Ninguna de estas opciones
6. ¿Cuál de los siguientes algoritmos es denominado AES?
7. Serpert
8. Rijdael
9. IDEA
10. DES
11. ¿Qué condiciona el libre uso de los algoritmos?
12. Ninguna de estas opciones
13. Que sean públicos
14. Que tengan patentes en vigencia
15. Que sean privadas
16. ¿Cuál de los siguientes elementos no corresponde a una función de negocio de SAMM?
17. Gobierno
18. Implementación
19. Verificación
20. Diseño
21. Construcción
22. ¿Cuál de los siguientes elementos NO corresponde a una característica positiva de los sistemas criptográficos simétricos?
23. Robustez
24. Velocidad de cifrado
25. Longitud del mensaje limitada por la implementación
26. Sencillez de implementación
27. ¿Cuál de los siguientes NO es un modo de cifrado de bloques?
28. CBC – Cipher Block Chaining
29. OFB – Output Feedback
30. CFB – Cipher Feedback
31. Ninguna de las opciones
32. ¿Cuál de las siguientes NO es una propiedad de la firma digital?
33. Va ligada indisolublemente al mensaje
34. Se genera en base a la clave pública del destinatario
35. Solo puede ser generada por su legitimo titular
36. Es públicamente verificable
37. ¿Qué significa el acrónimo CMM?
38. Capacity Model Metrics
39. Capability Maturity Model
40. Capability Model and Metrics
41. Capacity Measure Model
42. ¿Qué norma define la metodología de SCRUM?
43. Ninguna de las opciones
44. ISO 25000
45. ISO/IEC 9126
46. ISO/IEC 14598
47. Determine el mensaje original para el siguiente cifrado obtenido mediante el cifrado XOR solamente.

*VALOR CIFRADO*: 101110110010

*CONTRASEÑA* : 011100110110

Se conoce la existencia de los siguientes valores binarios 100111000011 y 11001111001

1. 101010100011
2. 110010000100
3. 001110110110
4. 111100111010
5. ¿A qué se denomina “Padding”
6. Al método para autenticar mensajes con algoritmos asimétricos
7. Al método para completar el inicio de un bloque de datos
8. Al método que permite generar una distorsión entre los distintos bloques
9. Al método para completar al final de un bloque de datos
10. ¿Cuál de los siguientes datos NO está contenido en los campos de un cifrado X509?
11. Número de serie
12. Nombre del sujeto
13. Clave privada del sujeto
14. Clave publica del sujeto
15. ¿Cuál de los siguientes puntos no es de interés para el manejo de sesiones de estado?
16. Seguridad de transporte
17. Ataque de autenticación de sesión
18. Paginas y credenciales en formularios
19. Entropia de credencial de sesión
20. ¿Cual de estos elementos no corresponde a la lista de requerimientos verificación de ASVS 2014?
21. Cryptography at Rest
22. Authentication
23. Data Protection
24. Communications
25. Mobile
26. Performance
27. Indique cuál de las definiciones correcta de J según la siguiente representación de un sistema criptográfico: **DJ (Ej (m)) = m**
28. Representa el conjunto de transformaciones de cifrado
29. Representa el conjunto de claves que se pueden emplear
30. Representa el conjunto de todos los mensajes sin cifrar
31. Representa el conjunto de todos los posibles mensajes cifrados
32. ¿Cuál de los siguientes elementos NO se corresponde con una propiedad de la Calidad en uso?
33. Productividad
34. Seguridad
35. Satisfacción
36. Eficacia
37. Ninguna de las opciones
38. ¿Qué establece el marco legal para el uso de la Firma Digital en la República Argentina?
39. El Pacto de San José de Costa Rica
40. La ley 25.506
41. La ley 24.449
42. La Constitución Nacional
43. ¿Qué característica de calidad Interna/Externa NO esta contemplada en SQuaRE?
44. Portabilidad
45. Mantenibilidad
46. Ninguna de estas opciones
47. Fiabilidad
48. ¿A que tipo de algoritmo corresponde el cifrado del Cesar?
49. Cifrado por transposición de grupos
50. Cifrado por sustitución
51. Cifrado asimétrico
52. Cifrado de simétrico de flujo
53. ¿Cuál de los siguientes puntos NO es objetivo de la administración de usuario y privilegios?
54. Los usuarios no pueden acceder o utilizar funcionalidades administrativas
55. Las funciones de nivel de administrador están segregadas apropiadamente de la actividad del usuario
56. Los usuarios transmiten información de manera cifrada y confidencial
57. Proveer la necesaria auditoria y trazabilidad de funcionalidad administrativa
58. ¿Cuál de estos elementos corresponde a la escala con que se representan los niveles de madurez de SAMM?
59. A, B, C
60. Bajo, Medio, Alto
61. 1, 2, 3, 4, 5, 6, 7, 8, 9, 10
62. 0, 1, 2, 3
63. ¿Sobre qué tecnología están desarrollados los Web Services?
64. XML/SOAP
65. HTTPS
66. AES
67. HTML
68. Indique a que corresponde la siguiente definición: “Se define como una función o método para generar un valor represente de manera casi univoca a un dato”
69. Función de encriptación de datos
70. Función de descifrado de datos
71. Función Hash
72. Función de firma digital
73. Indique cual es el orden creciente en base al nivel de seguridad de las siguientes técnicas de autenticación de usuario
74. Básica y segura, Basada en formas, Integrada, Fuerte, Basada en certificado
75. Basada en formas, Básicas y segura, Integrada, Fuerte, Basada en certificado
76. Básica y segura, Integrada, Basada en formas, Basada en certificado, Fuerte
77. Básica y segura, Basada en formas, Integrada, Basada en certificado, Fuerte
78. Basada en formas, Básica y segura, Integrada, Basada en certificado, Fuerte
79. ¿Cuál de estos elementos corresponde a un nivel que no define requerimientos detallados de verificación en ASVS?
80. Advanced
81. Cursory
82. Opportunistic
83. Standard
84. ¿Qué cantidad de PAs están definidos para el SSE-CMM?
85. 24
86. 16
87. 18
88. 22
89. ¿Qué modelo de autorización utiliza un sistema UNIX/Linux convencional para manejar sus archivos?
90. Mandatory Access Control (MAC)
91. Discretionary Access Control (DAC)
92. Role Based Access Control (RBAC)
93. Ninguna de estas opciones
94. Marque la respuesta correcta según indica el siguiente mensaje generado mediante el cifrado del Cesar: “od uhvsxhvwd fruuhfwd frqwlhqh od sdodeud ixhjr”
95. Los fideos tienen salsa
96. Hay estrellas en el cielo
97. La torre es demasiado alta
98. El fuego se apagara pronto
99. ¿Qué mecanismo adiciona criptografía al proceso de hash con el fin de incorporar autenticación a la seguridad del mismo?
100. MD5
101. MAC
102. AES
103. Ninguna de estas opciones
104. ¿Cuál de los siguientes algoritmos se basa en la dificultad para factorizar grandes números?
105. Ninguna de estas opciones
106. RSA
107. AES
108. ELGamal