Chapter 4 Review Questions

1. Which of the following is NOT a method for strengthening a key?
2. Randomness
3. Cryptoperiod
4. Length
5. Variability
6. Which of the following block ciphers XORs each block of plaintext with the previous block of ciphertext before being encrypted?
7. Electronic Code Book (ECB)
8. Galois/Counter (GCM)
9. Counter (CTR)
10. Cipher Block Chaining (CBC)
11. What entity calls in crypto modules to perform cryptographic tasks?
12. Certificate Authority (CA)
13. OCSP Chain
14. Intermediate CA
15. Crypto service provider
16. \_\_\_\_\_ are symmetric keys to encrypt and decrypt information exchanged during the session and to verify its integrity.
17. Encrypted signatures
18. Session keys
19. Digital certificates
20. Digital digests
21. Which of these is considered the strongest cryptographic transport protocol?
22. TLS v1.2
23. TLS v1.0
24. SSL v3.0
25. SSL v2.0
26. The strongest technology that would assure Alice that Bob is the sender of a message is a(n) \_\_\_\_\_.
27. digital signature
28. encrypted signature
29. digest
30. digital certificate
31. A digital certificate associates \_\_\_\_\_.
32. a user’s public key with his private key
33. the user’s identity with his public key
34. a user’s private key with the public key
35. a private key with a digital signature
36. Digital certificates can be used for each of these EXCEPT \_\_\_\_\_.
37. to verify the authenticity of the Registration Authorizer
38. to encrypt channels to provide secure communication between clients and servers
39. to verify the identity of clients and servers on the Web
40. to encrypt messages for secure email communications
41. An entity that issues digital certificates is a \_\_\_\_\_.
42. Certificate Signatory (CS)
43. Digital Signer (DS)
44. Certificate Authority (CA)
45. Signature Authority (SA)
46. A centralized directory of digital certificates is called a(n) \_\_\_\_\_.
47. Digital Signature Permitted Authorization (DSPA)
48. Digital Signature Approval List (DSAP)
49. Certificate Repository (CR)
50. Authorized Digital Signature (ADS)
51. \_\_\_\_\_ performs a real-time lookup of a digital certificate’s status.
52. Certificate Revocation List (CRL)
53. Real-Time CA Verification (RTCAV)
54. Online Certificate Status Protocol (OCSP)
55. CA Registry Database (CARD)
56. What is a value that can be used to ensure that hashed plaintext will not consistently result in the same digest?
57. algorithm
58. initialization vector (IV)
59. nonce
60. salt
61. Which digital certificate displays the name of the entity behind the website?
62. Online Certificate Status Certificate
63. Extended Validation (EV) Certificate
64. Session Certificate
65. X.509 Certificate
66. Which trust model has multiple CAs, one of which acts as a facilitator?
67. Bridge
68. Hierarchical
69. Distributed
70. Web
71. Which statement is NOT true regarding hierarchical trust models?
72. It is designed for use on a large scale.
73. The root signs all digital certificate authorities with a single key.
74. It assigns a single hierarchy with one master CA.
75. The master CA is called the root.
76. Public key infrastructure (PKI) \_\_\_\_\_.
77. generates public/private keys automatically
78. creates private key cryptography
79. is the management of digital certificates
80. requires the use of an RA instead of a CA
81. A(n) \_\_\_\_\_ is a published set of rules that govern the operation of a PKI.
82. signature resource guide (SRG)
83. enforcement certificate (EF)
84. certificate practice statement (CPS)
85. certificate policy (CP)
86. Which of these is NOT part of the certificate life cycle?
87. expiration
88. revocation
89. authorization
90. creation
91. \_\_\_\_\_ refers to a situation in which keys are managed by a third party, such as a trusted CA.
92. Key authorization
93. Key escrow
94. Remote key administration
95. Trusted key authority
96. \_\_\_\_\_ is a protocol for securely accessing a remote computer.
97. Transport Layer Security (TLS)
98. Secure Shell (SSH)
99. Secure Sockets Layer (SSL)
100. Secure Hypertext Transport Protocol (SHTTP)