Chapter 3 Review Questions

1. The Hashed Message Authentication Code (HMAC) \_\_\_\_\_.
2. encrypts only the message
3. encrypts only the key
4. encrypts the key and the message
5. encrypts the DHE key only
6. What is the latest version of the Secure Hash Algorithm?
7. SHA-2
8. SHA-3
9. SHA-4
10. SHA-5
11. Alexei was given a key to a substitution cipher. The key showed that the entire alphabet was rotated 13 steps. What type of cipher is this?
12. AES
13. XAND13
14. ROT13
15. Alphabetic
16. Abram was asked to explain to one of his coworkers the XOR cipher. He showed his coworker an example of adding two bits, 1 and 1. What is the result of this sum?
17. 2
18. 1
19. 0
20. 16
21. Which of the following key exchanges uses the same keys each time?
22. Diffie-Hellman-RSA (DHRSA)
23. Diffie-Hellman Ephemeral (DHE)
24. Diffie-Hellman (DH)
25. Elliptic Curve Diffie-Hellman (ECDH)
26. Public key systems that generate random public keys that are different for each session are called \_\_\_\_\_.
27. Public Key Exchange (PKE)
28. perfect forward secrecy
29. Elliptic Curve Diffie-Hellman (ECDH)
30. Diffie-Hellman (DH)
31. What is data called that is to be encrypted by inputting it into a cryptographic algorithm?
32. opentext
33. plaintext
34. cleartext
35. ciphertext
36. Which of these is NOT a basic security protection for information that cryptography can provide?
37. authenticity
38. risk loss
39. integrity
40. confidentiality
41. Which areas of a file *cannot* be used by steganography to hide data?
42. in areas that contain the content data itself
43. in the file header fields that describe the file
44. in data that is used to describe the content or structure of the actual data
45. in the directory structure of the file system
46. Proving that a user sent an email message is known as \_\_\_\_\_.
47. non-repudiation
48. repudiation
49. integrity
50. availability
51. A(n) \_\_\_\_\_ is not decrypted but is only used for comparison purposes.
52. key
53. stream
54. digest
55. algorithm
56. Which of these is NOT a characteristic of a secure hash algorithm?
57. Collisions should be rare.
58. A message cannot be produced from a predefined hash.
59. The results of a hash function should not be reversed.
60. The hash should always be the same fixed size.
61. Alyosha was explaining to a friend the importance of protecting a cryptographic key from cryptoanalysis. He said that the key should not relate in a simple way to the cipher text. Which protection is Alyosha describing?
62. diffusion
63. confusion
64. integrity
65. chaos
66. Which of these is the strongest symmetric cryptographic algorithm?
67. Data Encryption Standard
68. Triple Data Encryption Standard
69. Advanced Encryption Standard
70. RC 1
71. If Bob wants to send a secure message to Alice using an asymmetric cryptographic algorithm, which key does he use to encrypt the message?
72. Alice’s private key
73. Bob’s public key
74. Alice’s public key
75. Bob’s private key
76. Egor wanted to use a digital signature. Which of the following benefits will the digital signature not provide?
77. verify the sender
78. prove the integrity of the message
79. verify the receiver
80. enforce nonrepudiation
81. Illya was asked to recommend the most secure asymmetric cryptographic algorithm to his supervisor. Which of the following did he choose?
82. SHA-2
83. ME-312
84. BTC-2
85. RSA
86. At a staff meeting one of the technicians suggested that the enterprise protect its new web server by hiding it and not telling anyone where it is located. Iosif raised his hand and said that security through obscurity was a poor idea. Why did he say that?
87. It is an unproven approach and has never been tested.
88. It would be too costly to have one isolated server by itself.
89. It would be essentially impossible to keep its location a secret from everyone.
90. It depends too heavily upon non-repudiation in order for it to succeed.
91. What is a characteristic of the Trusted Platform Module (TPM)?
92. It provides cryptographic services in hardware instead of software
93. It allows the user to boot a corrupted disk and repair it
94. It is available only on Windows computers running BitLocker
95. It includes a pseudorandom number generator (PRNG)
96. Which of these has an onboard key generator and key storage facility, as well as accelerated symmetric and asymmetric encryption, and can back up sensitive material in encrypted form?
97. Trusted Platform Module (TPM)
98. Hardware Security Module (HSM)
99. self-encrypting hard disk drives (SED)
100. encrypted hardware-based USB devices