Module 6 Exam

1. **Each of the following is true about privacy EXCEPT: B**
2. Privacy is the right to be left alone to the degree that you choose.
3. Today individuals can achieve any level of privacy that is desired.
4. Privacy is difficult due to the volume of data silently accumulated by technology.
5. Privacy is freedom from attention, observation, or interference based on your decision.
6. **Which of the following is not a risk associated with the use of private data? B**
7. Individual inconveniences and identity theft.
8. Devices being infected with malware.
9. Associations with groups.
10. Statistical inferences.
11. **Which of the following is not an issue raised regarding how private data is gathered and used? C**
12. The data is gathered and kept in secret.
13. The accuracy of the data cannot be verified.
14. By law all encrypted data must contain a “backdoor” entry point.
15. Informed consent is usually missing or is misunderstood.
16. **\_\_\_D\_\_ hides the existence of the data.**
17. Cryptography
18. Symmetric encryption
19. Asymmetric decryption
20. Steganography
21. **What is ciphertext? C**
22. Procedures based on a mathematical formula used to encrypt and decrypt data.
23. A mathematical value entered into an algorithm.
24. Encrypted data.
25. The public key of a symmetric cryptographic process.
26. **Which of the following is “one-way” so that its contents cannot be used to reveal the original set of data? A**
27. hash
28. symmetric cryptography
29. Message Digest Encryption (MDE)
30. asymmetric cryptography
31. **What is data called that is to be encrypted by inputting it into a cryptographic algorithm? B**
32. ciphertext
33. plaintext
34. cleartext
35. opentext
36. **Which of these is NOT a basic security protection for information that cryptography can provide? A**
37. risk loss
38. authenticity
39. integrity
40. confidentiality
41. **The areas of a file in which steganography can hide data include all of the following EXCEPT \_B\_\_\_\_.**
42. in data that is used to describe the content or structure of the actual data
43. in the directory structure of the file system
44. in the file header fields that describe the file
45. in areas that contain the content data itself
46. **Proving that a user sent an email message is known as \_\_C\_\_\_.**
47. repudiation
48. integrity
49. nonrepudiation
50. availability
51. **A(n) \_\_\_B\_\_ is not decrypted but is only used for comparison purposes.**
52. stream
53. digest
54. algorithm
55. key
56. **Which of these is NOT a characteristic of a secure hash algorithm? B**
57. A message cannot be produced from a predefined hash.
58. Collisions should be rare.
59. The results of a hash function should not be reversed.
60. The hash should always be the same fixed size.
61. **How many keys are used in asymmetric cryptography? B**
62. One
63. Two
64. Three
65. Four
66. **Which of these is not a method for encryption through software? D**
67. Encrypt individual files
68. Whole disk encryption
69. Encrypt using the file system
70. Encrypt using a separate hardware computer chip
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? B**
72. Alice’s private key
73. Alice’s public key
74. Bob’s public key
75. Bob’s private key
76. **A digital signature can provide each of the following benefits EXCEPT \_\_\_B\_\_\_.**
77. prove the integrity of the message
78. verify the receiver
79. verify the sender
80. enforce nonrepudiation