|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 1. Encryption is the practice of transforming information so that it is secure and cannot be accessed by unauthorized parties.   |  |  |  | | --- | --- | --- | |  | a. | True | |  | b. | False |  |  |  | | --- | --- | | *ANSWER:* | False | |

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 2. Ciphertext is the scrambled and unreadable output of encryption.   |  |  |  | | --- | --- | --- | |  | a. | True | |  | b. | False |  |  |  | | --- | --- | | *ANSWER:* | True | |

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 3. The XOR cipher is based on the binary operation eXclusive OR that compares two bits.   |  |  |  | | --- | --- | --- | |  | a. | True | |  | b. | False |  |  |  | | --- | --- | | *ANSWER:* | True | |

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 4. In information technology, non-repudiation is the process of proving that a user performed an action.   |  |  |  | | --- | --- | --- | |  | a. | True | |  | b. | False |  |  |  | | --- | --- | | *ANSWER:* | True | |

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 5. Obfuscation is making something well known or clear.   |  |  |  | | --- | --- | --- | |  | a. | True | |  | b. | False |  |  |  | | --- | --- | | *ANSWER:* | False | |

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 6. One of the first popular symmetric cryptography algorithms was RSA.   |  |  |  | | --- | --- | --- | |  | a. | True | |  | b. | False |  |  |  | | --- | --- | | *ANSWER:* | False | |

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 7. Asymmetric cryptographic algorithms are also known as private key cryptography.   |  |  |  | | --- | --- | --- | |  | a. | True | |  | b. | False |  |  |  | | --- | --- | | *ANSWER:* | False | |

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 8. Wireless data networks are particularly susceptible to known ciphertext attacks.   |  |  |  | | --- | --- | --- | |  | a. | True | |  | b. | False |  |  |  | | --- | --- | | *ANSWER:* | True | |

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 9. A collision attack is an attempt to find two input strings of a hash function that produce the same hash result.   |  |  |  | | --- | --- | --- | |  | a. | True | |  | b. | False |  |  |  | | --- | --- | | *ANSWER:* | True | |

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 10. GNU Privacy Guard a proprietary software that runs on different operating systems.   |  |  |  | | --- | --- | --- | |  | a. | True | |  | b. | False |  |  |  | | --- | --- | | *ANSWER:* | False | |

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 11. What is a block cipher algorithm that operates on 64-bit blocks and can have a key length from 32 to 448 bits?   |  |  |  | | --- | --- | --- | |  | a. | Twofish | |  | b. | Blowfish | |  | c. | Whirlpool | |  | d. | Rijndal |  |  |  | | --- | --- | | *ANSWER:* | b | |

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 12. If using the MD5 hashing algorithm, what is the length to which each message is padded?   |  |  |  | | --- | --- | --- | |  | a. | 32 bits | |  | b. | 64 bits | |  | c. | 128 bits | |  | d. | 512 bits |  |  |  | | --- | --- | | *ANSWER:* | d | |

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 13. In which type of encryption is the same key used to encrypt and decrypt data?   |  |  |  | | --- | --- | --- | |  | a. | private | |  | b. | public | |  | c. | symmetric | |  | d. | asymmetric |  |  |  | | --- | --- | | *ANSWER:* | c | |

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 14. The simplest type of stream cipher, one in which one letter or character is exchanged for another, is known as what?   |  |  |  | | --- | --- | --- | |  | a. | shift | |  | b. | substitution | |  | c. | lock | |  | d. | loop |  |  |  | | --- | --- | | *ANSWER:* | b | |

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 15. Which type of cryptographic algorithm takes an input string of any length, and returns a string of any requested variable length?   |  |  |  | | --- | --- | --- | |  | a. | substitution | |  | b. | block | |  | c. | loop | |  | d. | sponge |  |  |  | | --- | --- | | *ANSWER:* | d | |

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 16. After the DES cipher was broken and no longer considered secure, what encryption algorithm was made as its successor?   |  |  |  | | --- | --- | --- | |  | a. | AES | |  | b. | Twofish | |  | c. | 3DES | |  | d. | RSA |  |  |  | | --- | --- | | *ANSWER:* | c | |

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 17. Which standard was approved by NIST in late 2000 as a replacement for DES?   |  |  |  | | --- | --- | --- | |  | a. | AES | |  | b. | 3DES | |  | c. | RSA | |  | d. | Twofish |  |  |  | | --- | --- | | *ANSWER:* | a | |

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 18. What type of cryptography uses two keys instead of just one, generating both a private and a public key?   |  |  |  | | --- | --- | --- | |  | a. | symmetric | |  | b. | asymmetric | |  | c. | shared | |  | d. | open |  |  |  | | --- | --- | | *ANSWER:* | b | |

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 19. Which of the following is not one of the functions of a digital signature?   |  |  |  | | --- | --- | --- | |  | a. | verification of the sender | |  | b. | prevention of the sender from disowning the message | |  | c. | prove the integrity of the message | |  | d. | protect the public key |  |  |  | | --- | --- | | *ANSWER:* | d | |

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 20. Which of the following asymmetric cryptography algorithms is most commonly used?   |  |  |  | | --- | --- | --- | |  | a. | AES | |  | b. | RSA | |  | c. | Twofish | |  | d. | Blowfish |  |  |  | | --- | --- | | *ANSWER:* | b | |

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 21. What cryptographic method, first proposed in the mid-1980s, makes use of sloping curves instead of large prime numbers?   |  |  |  | | --- | --- | --- | |  | a. | FCC | |  | b. | RSA | |  | c. | ECC | |  | d. | IKE |  |  |  | | --- | --- | | *ANSWER:* | c | |

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 22. What widely used commercial asymmetric cryptography software can be used for encrypting files and email messages?   |  |  |  | | --- | --- | --- | |  | a. | PGP | |  | b. | GPG | |  | c. | EFS | |  | d. | GNUPG |  |  |  | | --- | --- | | *ANSWER:* | a | |

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 23. The SHA-1 hashing algorithm creates a digest that is how many bits in length?   |  |  |  | | --- | --- | --- | |  | a. | 96 bits | |  | b. | 128 bits | |  | c. | 160 bits | |  | d. | 192 bits |  |  |  | | --- | --- | | *ANSWER:* | c | |

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 24. Data that is in an unencrypted form is referred to as which of the following?   |  |  |  | | --- | --- | --- | |  | a. | crypttext | |  | b. | plain text | |  | c. | simpletext | |  | d. | cleartext |  |  |  | | --- | --- | | *ANSWER:* | d | |

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 25. In cryptography, which of the five basic protections ensures that the information is correct and no unauthorized person or malicious software has altered that data?   |  |  |  | | --- | --- | --- | |  | a. | confidentiality | |  | b. | availability | |  | c. | encryption | |  | d. | integrity |  |  |  | | --- | --- | | *ANSWER:* | d | |

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 26. What type of cryptographic algorithm creates a unique digital fingerprint of a set of data?   |  |  |  | | --- | --- | --- | |  | a. | hash | |  | b. | key | |  | c. | digest | |  | d. | block |  |  |  | | --- | --- | | *ANSWER:* | a | |

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 27. Which hash algorithm's primary design feature is two different and independent parallel chains of computation, the results of which are then combined at the end of the process?   |  |  |  | | --- | --- | --- | |  | a. | SHA-384 | |  | b. | HMAC | |  | c. | RIPEMD | |  | d. | MD5 |  |  |  | | --- | --- | | *ANSWER:* | c | |

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 28. What type of cipher takes one character and replaces it with one character, working one character at a time?   |  |  |  | | --- | --- | --- | |  | a. | block cipher | |  | b. | single cipher | |  | c. | unit cipher | |  | d. | stream cipher |  |  |  | | --- | --- | | *ANSWER:* | d | |

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 29. What term describes data actions being performed by endpoint devices, such as printing a report from a desktop computer?   |  |  |  | | --- | --- | --- | |  | a. | data-in-transit | |  | b. | data-in-play | |  | c. | data-at-rest | |  | d. | data-in-use |  |  |  | | --- | --- | | *ANSWER:* | d | |

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 30. What type of message authentication code uses hashing to authenticate the sender by using both a hash function and a secret cryptographic key?   |  |  |  | | --- | --- | --- | |  | a. | SHA-384 | |  | b. | HMAC | |  | c. | RIPEMD | |  | d. | MD5 |  |  |  | | --- | --- | | *ANSWER:* | b | |

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 31. What alternative term can be used to describe asymmetric cryptographic algorithms?   |  |  |  | | --- | --- | --- | |  | a. | user key cryptography | |  | b. | public key cryptography | |  | c. | private key cryptography | |  | d. | cipher-text cryptography |  |  |  | | --- | --- | | *ANSWER:* | b | |

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 32. Which of the following are considered to be common asymmetric cryptographic algorithms? (Choose all that apply.)   |  |  |  | | --- | --- | --- | |  | a. | Data Encryption Standard | |  | b. | Elliptic Curve Cryptography | |  | c. | Advanced Encryption Standard | |  | d. | Digital Signature Algorithm |  |  |  | | --- | --- | | *ANSWER:* | b, d | |

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 33. What is the U.S. federal government standard for digital signatures?   |  |  |  | | --- | --- | --- | |  | a. | Data Encryption Standard | |  | b. | Elliptic Curve Cryptography | |  | c. | Advanced Encryption Standard | |  | d. | Digital Signature Algorithm |  |  |  | | --- | --- | | *ANSWER:* | d | |

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 34. If Bob receives an encrypted reply message from Alice, whose private key is used to decrypt the received message?   |  |  |  | | --- | --- | --- | |  | a. | Bob's private key. | |  | b. | Alice's private key. | |  | c. | Bob and Alice's keys. | |  | d. | Bob's private key and Alice's public key. |  |  |  | | --- | --- | | *ANSWER:* | a | |

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 35. When Bob needs to send Alice a message with a digital signature, whose private key is used to encrypt the hash?   |  |  |  | | --- | --- | --- | |  | a. | Bob's private key | |  | b. | Alice's private key | |  | c. | Bob and Alice's keys. | |  | d. | Bob's private key and Alice's public key. |  |  |  | | --- | --- | | *ANSWER:* | a | |

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 36. Which key exchange requires Alice and Bob to each agree upon a large prime number and related integer?   |  |  |  | | --- | --- | --- | |  | a. | Quantum Prime | |  | b. | Prime-Curve | |  | c. | Diffie-Hellman | |  | d. | Elliptic Curve Diffie-Hellman |  |  |  | | --- | --- | | *ANSWER:* | c | |

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 37. Which of the following is a public key system that generates random public keys that are different for each session?   |  |  |  | | --- | --- | --- | |  | a. | ephemeral-secrecy | |  | b. | perfect forward secrecy | |  | c. | public secrecy | |  | d. | random-key exchange |  |  |  | | --- | --- | | *ANSWER:* | b | |

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 38. What term best describes when cryptography is applied to entire disks instead of individual files or groups of files?   |  |  |  | | --- | --- | --- | |  | a. | full disk encryption | |  | b. | system encryption | |  | c. | OS encryption | |  | d. | disk encryption |  |  |  | | --- | --- | | *ANSWER:* | a | |

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 39. Which of the following is more secure than software encryption?   |  |  |  | | --- | --- | --- | |  | a. | hardware encryption | |  | b. | private encryption | |  | c. | application encryption | |  | d. | full disk encryption |  |  |  | | --- | --- | | *ANSWER:* | a | |

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 40. What technology uses a chip on the motherboard of the computer to provide cryptographic services?   |  |  |  | | --- | --- | --- | |  | a. | SEDs | |  | b. | FDE | |  | c. | TPM | |  | d. | HSM |  |  |  | | --- | --- | | *ANSWER:* | c | |

|  |  |  |
| --- | --- | --- |
| 41. Explain how a hash algorithm works and how it is primarily used.   |  |  | | --- | --- | | *ANSWER:* | A hash algorithm creates a unique "digital fingerprint" of a set of data. This process is called hashing, and the resulting fingerprint is a digest (sometimes called a message digest or hash) that represents the contents. Hashing is used primarily for comparison purposes. | |

|  |  |  |
| --- | --- | --- |
| 42. What is a pseudorandom number generator?   |  |  | | --- | --- | | *ANSWER:* | A pseudorandom number generator is an algorithm for creating a sequence of numbers whose properties approximate those of a random number. | |

|  |  |  |
| --- | --- | --- |
| 43. What four basic protections can cryptography support?   |  |  | | --- | --- | | *ANSWER:* | Cryptography can support confidentiality, integrity, authentication, and non-repudiation. | |

|  |  |  |
| --- | --- | --- |
| 44. What is meant by the phrase "security through obscurity," and why is this concept not accurate?   |  |  | | --- | --- | | *ANSWER:* | Security through obscurity, or the notion that virtually any system can be made secure so long as outsiders are unaware of it or how it functions. However, this is a flawed approach since it is essentially impossible to keep "secrets" from everyone. | |

|  |  |  |
| --- | --- | --- |
| 45. What is the difference between a stream cipher and a block cipher?   |  |  | | --- | --- | | *ANSWER:* | When comparing the amount of data a cryptographic algorithm process, a stream cipher works on one character at a time and a block cipher manipulates an entire block of plaintext at one time. | |

|  |  |  |
| --- | --- | --- |
| 46. What characteristics are needed to consider a hashing algorithm secure?   |  |  | | --- | --- | | *ANSWER:* | The hashing algorithm must be a fixed size and unique, original, and secure. | |

|  |  |  |
| --- | --- | --- |
| 47. What is the Advanced Encryption Standard (AES)?   |  |  | | --- | --- | | *ANSWER:* | The Advanced Encryption Standard (AES) is a symmetric cipher that was approved by the NIST in late 2000 as a replacement for DES. AES performs three steps on every block (128 bits) of plaintext. Within step 2, multiple rounds are performed depending upon the key size: a 128-bit key performs 9 rounds, a 192-bit key performs 11 rounds, and a 256-bit key, known as AES-256, uses 13 rounds. Within each round, bytes are substituted and rearranged, and then special multiplication is performed based on the new arrangement. To date, no attacks have been successful against AES. | |

|  |  |  |
| --- | --- | --- |
| 48. How does asymmetric encryption work?   |  |  | | --- | --- | | *ANSWER:* | Asymmetric encryption uses two keys instead of only one. These keys are mathematically related and are called the public key and the private key. The public key is known to everyone and can be freely distributed, while the private key is known only to the individual to whom it belongs. When Bob wants to send a secure message to Alice, he uses Alice's public key to encrypt the message. Alice then uses her private key to decrypt it. | |

|  |  |  |
| --- | --- | --- |
| 49. What is Elliptic curve cryptography?   |  |  | | --- | --- | | *ANSWER:* | Elliptic curve cryptography (ECC) was first proposed in the mid-1980s. Instead of using large prime numbers as with RSA, elliptic curve cryptography uses sloping curves. An elliptic curve is a function drawn on an X-Y axis as a gently curved line. By adding the values of two points on the curve, a third point on the curve can be derived, of which the inverse is used. | |

|  |  |  |
| --- | --- | --- |
| 50. How does a downgrade attack work?   |  |  | | --- | --- | | *ANSWER:* | In a downgrade attack a threat actor forces the system to abandon the current higher security mode of operation and instead "fall back" to implementing an older and less secure mode. This then allows the threat actor to attack the weaker mode. | |