**崑山科技大學資工系IPAS證照輔導班 練習**

**名稱:** *CompTIA SecurityPLUS\_Ch6\_* Cryptography\_and\_PKI

|  |  |  |
| --- | --- | --- |
|  | | |
| 答案 | 編號 | 題目 |
|  | 1. | Which of the following would a public key be used for?  **A.** To decrypt a hash of a digital signature  **B.** To encrypt TLS traffic  **C.** To digitally sign messages  **D.** To decrypt TLS messages |
|  | 2. | Your company’s web server certificate has been revoked and external customers are receiving errors when they connect to the website. Which of following actions must you take?  **A.** Renew the certificate.  **B.** Create and use a self-signed certificate.  **C.** Request a certificate from the key escrow.  **D.** Generate a new key pair and new certificate |
|  | 3. | Mary is concerned about the validity of an email because a coworker denies sending it. How can Mary prove the authenticity of the email? **A.** Symmetric algorithm **B.** Digital signature  **C.** CRL **D.** Asymmetric algorithm |
|  | 4. | . Wi-Fi Alliance recommends that a passphrase be how many characters in length for WPA2-Personal security?  **A.** 6 characters **B.** 8 characters  **C.** 12 characters **D.** 16 characters |
|  | 5. | Which of the following digital certificate management practices will ensure that a lost certificate is not compromised?  **A.** CRL **B.** Key escrow  **C.** Nonrepudiation **D.** Recovery agent |
|  | 6. | Which of the following are restricted to 64-bit block sizes? (Choose two.)  **A.** DES **B.** SHA **C.** MD5 **D.** 3DES |
|  | 7. | Your company has implemented a RADIUS server and has clients that are capable of using multiple EAP types, including one configured for use on the RADIUS server. Your security manager wants to implement a WPA2-Enterprise system. Since you have the RADIUS server and clients, what piece of the network would you need?  **A.** Network access control **B.** Authentication server  **C.** Authenticator **D.** Supplicant |
|  | 8. | You are given the task of selecting an asymmetric encryption type that has an appropriate level of encryption strength but uses a smaller key length than is typically required. Which of the following encryption methods will accomplish your requirement?  **A.** Blowfish **B.** RSA **C.** DHE **D.** ECC |
|  | 9. | Matt has been told that successful attacks have been taking place and data that has been encrypted by his company’s software system has leaked to the company’s competitors. Matt, through investigation, has discovered patterns due to the lack of randomness in the seeding values used by the encryption algorithm in the company’s software. This discovery has led to successful reverse engineering. What can the company use to ensure patterns are not created during the encryption process?  **A.** One-time pad **B.** Initialization vector  **C.** Stream cipher **D.** Block cipher |
|  | 10. | You are asked to configure a WLAN that does not require a user to provide any credentials to associate with a wireless AP and access a WLAN. What type of authentication is said to be in use?  **A.** IV **B.** WEP **C.** WPA **D.** Open |
|  | 11. | The CIO at your company no longer wants to use asymmetric algorithms because of the cost. Of the following algorithms, which should the CIO discontinue using?  **A.** AES **B.** RC4 **C.** RSA **D.** Twofish |
|  | 12. | Which of the following would you use to verify certificate status by receiving a response of “good,” “revoked,” or “unknown”?  **A.** CRL **B.** OSCP **C.** RA **D.** PKI |
|  | 13. | Which of the following symmetric key algorithms are block ciphers? (Choose two.)  **A.** MD5 **B.** 3DES **C.** RC4 **D.** Blowfish |
|  | 14. | Which of the following encryption algorithms is the weakest?  **A.** Blowfish **B.** AES **C.** DES **D.** SHA |
|  | 15. | What encryption protocol does WEP improperly use?  **A.** RC6 **B.** RC4 **C.** AES **D.** DES |
|  | 16. | James, an IT manager, expresses a concern during a monthly meeting about weak user passwords used on company servers and how they may be susceptible to brute-force password attacks. Which concept can James implement to make the weak passwords stronger?  **A.** Key stretching **B.** Key escrow  **C.** Key strength **D.** ECC |
|  | 17. | You are installing a network for a small business named Matrix Interior Design that the owner is operating out of their home. There are only four devices that will use the wireless LAN, and you are installing a SOHO wireless router between the wireless LAN clients and the broadband connection. To ensure better security from outside threats connecting to the wireless SOHO router, which of the following would be a good choice for the WPA2-PSK passphrase?  **A.** 123456 **B.** XXrcERr6Euex9pRCdn3h3  **C.** bRtlBv **D.** HomeBusiness |
|  | 18. | You set up your wireless SOHO router to encrypt wireless traffic, and you configure the router to require wireless clients to authenticate against a RADIUS server. What type of security have you configured?  **A.** WPA2 Enterprise **B.** WPA2 Personal  **C.** TKIP **D.** WEP |
|  | 19. | You must implement a cryptography system that applies encryption to a group of data at a time. Which of the following would you choose?  **A.** Stream **B.** Block  **C.** Asymmetric **D.** Symmetric |
|  | 20. | Which symmetric block cipher supersedes Blowfish?  **A.** RSA **B.** Twofish  **C.** MD5 **D.** PBKDF2 |
|  | 21. | Root CAs can delegate their authority to which of the following to issue certificates to users?  **A.** Registered authorities **B.** Intermediate CAs  **C.** CRL **D.** CSR |
|  | 22. | Which of the following protocols should be used to authenticate remote access users with smartcards?  **A.** PEAP **B.** EAP-TLS **C.** CHAP **D.** MS-CHAPv2 |
|  | 23. | Tom is sending Mary a document and wants to show the document came from him. Which of the following should Tom use to digitally sign the document?  **A.** TKIP **B.** Intermediate CA  **C.** Public key **D.** Private key |
|  | 24. | Which of the following EAP types offers support for legacy authentication protocols such as PAP, CHAP, MS-CHAP, or MS-CHAPv2? **A.** PEAP **B.** EAP-FAST **C.** EAP-TLS **D.** EAP-TTLS |
|  | 25. | You are conducting a training program for new network administrators for your company. You talk about the benefits of asymmetric encryption. Which of the following are considered asymmetric algorithms? (Choose two.)  **A.** RC4 **B.** DES **C.** RSA **D.** ECC |
|  | 26. | Which of the following is a form of encryption also known as ROT13?  **A.** Substitution cipher **B.** Transposition cipher  **C.** Diffusion **D.** Confusion |
|  | 27. | Matt needs to calculate the number of keys that must be generated for 480 employees using the company’s PKI asymmetric algorithm. How many keys must Matt create?  **A.** 114,960 **B.** 480 **C.** 960 **D.** 229,920 |
|  | 28. | You are conducting a one-time electronic transaction with another company. The transaction needs to be encrypted, and for efficiency and simplicity, you want to use a single key for encryption and decryption of the data. Which of the following types would you use?  **A.** Asymmetric **B.** Symmetric  **C.** Hashing **D.** Steganography |
|  | 29. | Which of the following uses two mathematically related keys to secure data during transmission?  **A.** Twofish **B.** 3DES **C.** RC4 **D.** RSA |
|  | 30. | You have been instructed by the security manager to protect the server’s data-at-rest. Which of the following would provide the strongest protection?  **A.** Implement a full-disk encryption system.  **B.** Implement biometric controls on data entry points.  **C.** Implement a host-based intrusion detection system.  **D.** Implement a host-based intrusion prevention system |
|  | 31. | Which of the following EAP types use a three-phase operation?  **A.** EAP-FAST **B.** EAP-TLS  **C.** EAP-TTLS **D.** PEAP |
|  | 32. | Which of the following is an encryption standard that uses a single 56-bit symmetric key?  **A.** DES **B.** 3DES **C.** AES **D.** WPS |
|  | 33. | Which of the following cryptography concepts converts output data into a fixed-length value and cannot be reversed?  **A.** Steganography **B.** Hashing **C.** Collision **D.** IV |
|  | 34. | SSL is a protocol used for securing transactions transmitting over an untrusted network such as the Internet. Which of the following best describes the action that occurs during the SSL connection setup process?  **A.** The client creates a session key and encrypts it with the server’s private key.  **B.** The client creates a session key and encrypts it with the server’s public key.  **C.** The server creates a session key and encrypts it with the client’s private key.  **D.** The server creates a session key and encrypts it with the client’s public key |
|  | 35. | Which of the following EAP types requires both server and client certificates?  **A.** EAP-FAST **B.** PEAP **C.** EAP-TLS **D.** EAP-TTLS |
|  | 36. | You are the network administrator for a small office of 35 users and need to utilize mail encryption that will allow specific users to encrypt outgoing email messages. You are looking for an inexpensive onsite encryption server. Which of the following would you implement?  **A.** PGP/GPG **B.** WPA2 **C.** CRL **D.** EAP-TLS |
|  | 37. | You have been promoted to security administrator for your company and you need to be aware of all types of hashing algorithms for integrity checks. Which algorithm offers a 160-bit digest?  **A.** MD5 **B.** RC4 **C.** SHA-1 **D.** AES |
|  | 38. | You are the security manager for your company, and a system administrator wants to know if there is a way to reduce the cost of certificates by purchasing a certificate to cover all domains and subdomains for the company. Which of the following solutions would you offer?  **A.** Wildcards **B.** Object identifiers  **C.** Key escrow **D.** OCSP |
|  | 39. | Which of the following are authentication protocols? (Choose two.)  **A.** WPS **B.** EAP **C.** IPSec **D.** IEEE 802.1x |
|  | 40. | Your company is looking to accept electronic orders from a vendor and wants to ensure nonauthorized people cannot send orders. Your manager wants a solution that provides nonrepudiation. Which of the following options would meet the requirements?  **A.** Digital signatures **B.** Hashes  **C.** Steganography **D.** Perfect forward secrecy |
|  | 41. | You are tasked to implement a solution to ensure data that are stored on a removable USB drive hasn’t been tampered with. Which of the following would you implement?  **A.** Key escrow **B.** File backup  **C.** File encryption **D.** File hashing |
|  | 42. | Which of the following is mainly used for remote access into a network?  **A.** TACACS+ **B.** XTACACS  **C.** Kerberos **D.** RADIUS |
|  | 43. | A security manager has asked you to explain why encryption is important and what symmetric encryption offers. Which of the following is the best explanation?  **A.** Confidentiality **B.** Nonrepudiation  **C.** Steganography **D.** Collision |
|  | 44. | You are a security administrator and have discovered one of the employees has been encoding confidential information into graphic files. Your employee is sharing these pictures on their social media account. What concept was the employee using?  **A.** Hashing **B.** Steganography  **C.** Symmetric algorithm **D.** Asymmetric algorithm |
|  | 45. | Your company’s branch offices connect to the main office through a VPN. You recently discovered the key used on the VPN has been compromised. What should you do to ensure the key isn’t compromised in the future?  **A.** Enable perfect forward secrecy at the main office and branch office ends of the VPN.  **B.** Enable perfect forward secrecy at the main office end of the VPN.  **C.** Enable perfect forward secrecy at the branch office end of the VPN. **D.** Disable perfect forward secrecy at the main office and branch office ends of the VPN. |
|  | 46. | You are configuring your friend’s new wireless SOHO router and discover a PIN on the back of the router. Which of the following best describes the purpose of the PIN?  **A.** This is a WEP PIN. **B.** This is a WPS PIN.  **C.** This is a WPA PIN. **D.** This is a Bluetooth PIN |
|  | 47. | Which of the following benefits do digital signatures provide? (Choose two.)  **A.** Nonrepudiation **B.** Authentication  **C.** Encryption **D.** Key exchange |
|  | 48. | Your company has asked you to recommend a secure method for password storage. Which of the following would provide the best protection against brute-force attacks? (Choose two.)  **A.** ROT13 **B.** MD5 **C.** PBKDF2 **D.** BCRYPT |
|  | 49. | Your IT support center is receiving a high number of calls stating that users trying to access the company’s website are receiving certificate errors within their browsers. Which of the following statements best describes what the issue is?  **A.** The website certificate has expired.  **B.** Users have forgotten their usernames or passwords.  **C.** The domain name has expired.  **D.** The network is currently unavailable |
|  | 50. | In asymmetric encryption, what is used to decrypt an encrypted file?  **A.** Private key **B.** Public key  **C.** Message digest **D.** Ciphertext |
|  | 51. | You are performing a vulnerability assessment on a company’s LAN and determine they are using 802.1x for secure access. Which of the following attacks can a threat actor use to bypass the network security?  **A.** MAC spoofing **B.** ARP poisoning  **C.** Ping of death **D.** Xmas attack |
|  | 52. | Your security manager is looking to implement a one-time pad scheme for the company’s salespeople to use when traveling. Which of the following best describes a requirement for this implementation? (Choose three.)  **A.** The pad must be distributed securely and protected at its destination.  **B.** The pad must always be the same length.  **C.** The pad must be used only one time.  **D.** The pad must be made up of truly random values |
|  | 53. | A threat actor has created a man-in-the-middle attack and captured encrypted communication between two users. The threat actor was unable to decrypt the messages. Which of the following is the reason the threat actor is unable to decrypt the messages?  **A.** Hashing **B.** Symmetric encryption  **C.** Asymmetric encryption **D.** Key escrow |
|  | 54. | You have implemented a PKI to send signed and encrypted data. The user sending data must have which of the following? (Choose two.)  **A.** The receiver’s private key **B.** The sender’s private key  **C.** The sender’s public key **D.** The receiver’s public key |
|  | 55. | Which of the following best describes the drawback of symmetric key systems?  **A.** You must use different keys for encryption and decryption.  **B.** The algorithm is more complex.  **C.** The system works much more slowly than an asymmetric system.  **D.** The key must be delivered in a secure manner. |
|  | 56. | Your company is looking for a secure backup mechanism for key storage in a PKI. Which of the following would you recommend?  **A.** CSR **B.** Key escrow **C.** CRL **D.** CA |
|  | 57. | Which cryptography concept uses points on a curve to define public and private key pairs?  **A.** Obfuscation **B.** ECC **C.** Stream cipher **D.** Block cipher |
|  | 58. | You are a security administrator and have been given instructions to update the access points to provide a more secure connection. The access points are currently set to use WPA TKIP for encryption. Which of the following would you configure to accomplish the task of providing a more secure connection?  **A.** WEP **B.** WPA2 CCMP  **C.** Enable MAC filtering **D.** Disable SSID broadcast |
|  | 59. | Which of the following is an example of a stream cipher?  **A.** AES **B.** DES **C.** 3DES **D.** RC4 |
|  | 60. | Which of the following are negotiation protocols commonly used by TLS? (Choose two.) **A.** DHE **B.** ECDHE **C.** RSA **D.** SHA |
|  | 61. | Which of the following statements is true regarding symmetric key systems?  **A.** They use different keys on each end of the transported data.  **B.** They use public key cryptography.  **C.** They use multiple keys for creating digital signatures.  **D.** They use the same key on each end of the transported data. |
|  | 62. | Which of the following ciphers was created from the foundation of the Rijndael algorithm?  **A.** TKIP **B.** AES **C.** DES **D.** 3DES |
|  | 63. | Katelyn is sending an important email to Zackary, the manager of human resources. Company policy states messages to human resources must be digitally signed. Which of the following statements is correct?  **A.** Katelyn’s public key is used to verify the digital signature.  **B.** Katelyn’s private key is used to verify the digital signature.  **C.** Zackary’s public key is used to verify the digital signature.  **D.** Zackary’s private key is used to verify the digital signature |
|  | 64. | Data integrity is provided by which of the following?  **A.** 3DES **B.** MD5 **C.** AES **D.** Blowfish |
|  | 65. | Which of the following is a symmetric encryption algorithm that is available in 128-bit, 192-bit, and 256-bit key versions?  **A.** AES **B.** DES **C.** RSA **D.** TKIP |
|  | 66. | Which of the following items are found within a digital certificate? (Choose two.)  **A.** Serial number **B.** Default gateway  **C.** Public key **D.** Session key |
|  | 67. | In an 802.1x implementation, which of the following devices mutually authenticate with each other? (Choose two.)  **A.** Authentication server **B.** Certificate authority  **C.** Domain controller **D.** Supplicant |
|  | 68. | Which of the following statements is true regarding the confusion encryption method?  **A.** It puts one item in the place of another; for example, one letter for another or one letter for a number.  **B.** It scrambles data by reordering the plain text in a certain way.  **C.** It uses a relationship between the plain text and the key that is so complicated the plain text can’t be altered and the key can’t be determined.  **D.** Change in the plain text will result in multiple changes that are spread throughout the cipher text. |
|  | 69. | Which of the following is required when employing PKI and preserving data is important?  **A.** CA **B.** CRL **C.** Key escrow **D.** CER |
|  | 70. | You need to encrypt the signature of an email within a PKI system. Which of the following would you use?  **A.** CER **B.** Public key  **C.** Shared key **D.** Private key |
|  | 71. | Which of the following standards was developed by the Wi-Fi Alliance and implements the requirements of IEEE 802.11i?  **A.** NIC **B.** WPA **C.** WPA2 **D.** TKIP |
|  | 72. | You are asked to create a wireless network for your company that implements a wireless protocol that provides maximum security while providing support for older wireless devices. Which protocol should you use?  **A.** WPA **B.** WPA2 **C.** WEP **D.** IV |
|  | 73. | Bob is a security administrator and needs to encrypt and authenticate messages that are sent and received between two systems. Which of the following would Bob choose to accomplish his task?  **A.** Diffie-Hellman **B.** MD5 **C.** SHA-256 **D.** RSA |
|  | 74. | Which of the following algorithms is generally used in mobile devices? **A.** 3DES **B.** DES **C.** ECC **D.** AES |
|  | 75. | Which of the following statements best describes the difference between public key cryptography and public key infrastructure?  **A.** Public key cryptography is another name for an asymmetric algorithm, whereas public key infrastructure is another name for a symmetric algorithm.  **B.** Public key cryptography uses one key to encrypt and decrypt the data, and public key infrastructure uses two keys to encrypt and decrypt the data.  **C.** Public key cryptography is another name for asymmetric cryptography, whereas public key infrastructure contains the public key cryptographic mechanisms.  **D.** Public key cryptography provides authentication and nonrepudiation, whereas public key infrastructure provides confidentiality and integrity. |
|  | 76. | Your company has a public key infrastructure (PKI) in place to issue digital certificates to users. Recently, your company hired temporary contractors for a project that is now complete. Management has requested that all digital certificates issued to the contractors be revoked. Which PKI component would you consult for the management’s request?  **A.** CA **B.** CRL **C.** RA **D.** CSR |
|  | 77. | Which of the following security setup modes are intended for use in a small office or home office environment? (Choose two.)  **A.** WPS **B.** WPA-Enterprise  **C.** WPA2-Enterprise **D.** WPA2-Personal |
|  | 78. | Which of the following automatically updates browsers with a list of root certificates from an online source to track which certificates are to be trusted?  **A.** Trust model **B.** Key escrow **C.** PKI **D.** RA |
|  | 79. | Which of the following EAP types uses the concepts of public key infrastructure (PKI)?  **A.** EAP-TLS **B.** PEAP **C.** EAP-FAST **D.** EAP-TTLS |
|  | 80. | Which of the following use PSK authentication? (Choose two.)  **A.** WPA-Enterprise **B.** WPA-Personal  **C.** WPA2-Personal **D.** WPA2-Enterprise |
|  | 81. | You are receiving calls from users who are connected to the company’s network and are being redirected to a login page with the company’s logo after they type a popular social media web address in an Internet browser. Which of the following is causing this to happen?  **A.** WEP **B.** Key stretching  **C.** MAC filtering **D.** Captive portal |
|  | 82. | Elliptic curve cryptosystem (ECC) is an asymmetric algorithm. Which of the following statements best describe why ECC is different from other asymmetric algorithms? (Choose two.)  **A.** It is more efficient.  **B.** It provides digital signatures, secure key distribution, and encryption.  **C.** It uses more processing power to perform encryption.  **D.** It provides fast key generation. |
|  | 83. | WEP’s RC4 approach to encryption uses a 24-bit string of characters added to data that are transmitted. The same plain text data frame will not appear as the same WEPencrypted data frame. What is this string of characters called?  **A.** Diffusion **B.** IV **C.** Session key **D.** Hashing |
|  | 84. | Your manager has recently purchased a RADIUS server that will be used by remote employees to connect to internal resources. Several client computers need to connect to the RADIUS server in a secure manner. What should your manager deploy?  **A.** HIDS **B.** UTM **C.** VLAN **D.** 802.1x |
|  | 85. | Katelyn, a network administrator, has deleted the account for a user who left the company last week. The user’s files were encrypted with a private key. How can Katelyn view the user’s files?  **A.** The data can be decrypted using the backup user account.  **B.** The data can be decrypted using the recovery agent.  **C.** She must re-create the former user’s account.  **D.** The data can be decrypted using a CRL |
|  | 86. | Your company has recently implemented an encryption system on the network. The system uses a secret key between two parties and must be kept secret. Which system was implemented?  **A.** Asymmetric algorithm **B.** Symmetric algorithm  **C.** Hashing algorithm **D.** Steganography |
|  | 87. | Tim, a wireless administrator, has been tasked with securing the company’s WLAN. Which of the following cryptographic protocols would Tim use to provide the most secure environment for the company?  **A.** WPA2 CCMP **B.** WEP **C.** WPA **D.** WPA2 TKIP |
|  | 88. | Which of the following defines a hashing algorithm creating the same hash value from two different messages?  **A.** AES **B.** MD5 **C.** Hashing **D.** Collision |
|  | 89. | Matt, a network administrator, is deciding which credential-type authentication to use within the company’s planned 802.1x deployment. He is searching for a method that requires a client certificate and a server-side certificate, and that uses tunnels for encryption. Which credential-type authentication method would Matt use?  **A.** EAP-TLS **B.** EAP-FAST **C.** PEAP **D.** EAP |
|  | 90. | A coworker is connecting to a secure website using HTTPS. The coworker informs you that before the website loads, their web browser displays an error indicating that the site certificate is invalid and the site is not trusted. Which of the following is most likely the issue?  **A.** The web browser is requiring an update.  **B.** The server is using a self-signed certificate.  **C.** A web proxy is blocking the connection.  **D.** The web server is currently unavailable. |
|  | 91. | Zack, an administrator, needs to renew a certificate for the company’s web server. Which of the following would you recommend Zack submit to the CA?  **A.** CSR **B.** Key escrow **C.** CRL **D.** OCSP |
|  | 92. | Which of the following types of encryption offers easy key exchange and key management?  **A.** Obfuscation **B.** Asymmetric  **C.** Symmetric **D.** Hashing |
|  | 93. | Which of the following is used to exchange cryptographic keys?  **A.** Diffie-Hellman **B.** HMAC **C.** ROT13 **D.** RC4 |
|  | 94. | Which of the following encryption algorithms is used to encrypt and decrypt data?  **A.** MD5 **B.** HMAC **C.** Kerberos **D.** RC4 |
|  | 95. | Which of the following provides additional encryption strength by repeating the encryption process with additional keys?  **A.** 3DES **B.** AES **C.** Twofish **D.** Blowfish |
|  | 96. | Which of the following security mechanisms can be used for the purpose of nonrepudiation?  **A.** Encryption **B.** Digital signature  **C.** Collision **D.** CA |
|  | 97. | You are a network administrator for your company, and the single AP that allows clients to connect to the wireless LAN is configured with a WPA-PSK preshared key of the company name followed by the number 1. Which of the following statements is correct regarding this implementation?  **A.** It is secure because WPA-PSK resolved the problem with WEP.  **B.** It is secure because the preshared key is at least five characters long. **C.** It is not secure because the preshared key includes only one number 　　　　　 and the company name so it can be easily guessed.  **D.** It is not secure because WPA-PSK is as insecure as WEP and should never be used. |
|  | 98. | You are a security technician and have been given the task to implement a PKI on the company’s network. When verifying the validity of a certificate, you want to ensure bandwidth isn’t consumed. Which of the following can you implement?  **A.** CRL **B.** OCSP **C.** Key escrow **D.** CA |
|  | 99. | Which of the following types of device are found in a network that supports Wi-Fi Protected Setup (WPS) protocol? (Choose three.)  **A.** Registrar **B.** Supplicant  **C.** Enrollee **D.** Access Point |
|  | 100. | You are a network administrator for a distribution company and the manager wants to implement a secure wireless LAN for a BYOD policy. Through research, you determine that the company should implement AES encryption and the 802.1x authentication protocol. You also determine that too many APs and clients will be installed and you will need to configure each one with a preshared key passphrase. Which of the following will meet your needs?  **A.** WEP **B.** WPA  **C.** WPA2-Personal **D.** WPA2-Enterprise |
|  | 101. | The process of deleting data by sending a single erase or clear instruction to an address of the nonvolatile memory is an example of securing which of the following?  **A.** Data-in-transit **B.** Data-over-the-network  **C.** Data-in-use **D.** Data-at-rest |
|  | 102. | Which of the following is an authentication service and uses UDP as a transport medium?  **A.** TACACS+ **B.** RADIUS **C.** LDAP **D.** Kerberos |
|  | 103. | Which of the following is true regarding the importance of encryption of data-at-rest for sensitive information?  **A.** It renders the recovery of data more difficult should the user lose their password.  **B.** It allows the user to verify the integrity of the data on the stored device.  **C.** It prevents the sensitive data from being accessed after a theft of the physical equipment.  **D.** It renders the recovery of data easier should the user lose their password. |
|  | 104. | You are a network administrator and your manager has asked you to enable WPA2 CCMP for wireless clients, along with an encryption to protect the data transmitting across the network. Which of the following encryption methods would you use along with WPA2 CCMP? **A.** RC4 **B.** DES **C.** AES **D.** 3DES |
|  | 105. | Which of the following is the least secure hashing algorithm?  **A.** MD5 **B.** RIPEMD **C.** SHA-1 **D.** AES |
|  | 106. | Which of the following types of attack sends two different messages using the same hash function, causing a collision?  **A.** Xmas attack **B.** DoS  **C.** Logic bomb **D.** Birthday attack |
|  | 107. | Which of the following defines a file format commonly used to store private keys with associated public key certificates?  **A.** PKCS #1 **B.** PKCS #3 **C.** PKCS #7 **D.** PKCS #12 |
|  | 108. | Which of the following statements are true regarding ciphers? (Choose two.)  **A.** Stream ciphers encrypt fixed sizes of data.  **B.** Stream ciphers encrypt data one bit at a time.  **C.** Block ciphers encrypt data one bit at a time.  **D.** Block ciphers encrypt fixed sizes of data. |
|  | 109. | How many effective key sizes of bits does 3DES have? (Choose three.) **A.** 56 **B.** 112 **C.** 128 **D.** 168 |
|  | 110. | Which of the following statements is true about symmetric algorithms? **A.** They hide data within an image file.  **B.** They use one key to encrypt data and another to decrypt data.  **C.** They use a single key to encrypt and decrypt data.  **D.** They use a single key to create a hashing value. |
|  | 111. | The CA is responsible for revoking certificates when necessary. Which of the following statements best describes the relationship between a CRL and OSCP?  **A.** OCSP is a protocol to submit revoked certificates to a CRL.  **B.** CRL is a more streamlined approach to OCSP.  **C.** CRL validates a certificate in real time and reports it to the OCSP.  **D.** OCSP is a protocol to check the CRL during a certificate validation process. |
|  | 112. | Which of the following takes each bit in a character and is XORed with the corresponding bit in the secret key?  **A.** ECDHE **B.** PBKDF2  **C.** Obfuscation **D.** One-time pad |
|  | 113. | Which of the following works similarly to stream ciphers?  **A.** One-time pad **B.** RSA **C.** AES **D.** DES |
|  | 114. | Your manager wants to implement a security measure to protect sensitive company data that reside on the remote salespeople’s laptops should they become lost or stolen. Which of the following measures would you implement?  **A.** Implement WPS on the laptops.  **B.** Set BIOS passwords on the laptops.  **C.** Use whole-disk encryption on the laptops.  **D.** Use cable locks on the laptops. |
|  | 115. | You want to send confidential messages to a friend through email, but you do not have a way of encrypting the message. Which of the following methods would help you achieve this goal?  **A.** AES **B.** Collision  **C.** RSA **D.** Steganography |
|  | 116. | Which of the following cipher modes uses a feedback-based encryption method to ensure that repetitive data result in unique cipher text?  **A.** ECB **B.** CBC **C.** GCM **D.** CTM |
|  | 117. | Which statement is true regarding the difference between a secure cipher and a secure hash?  **A.** A secure hash can be reversed; a secure cipher cannot.  **B.** A secure cipher can be reversed; a secure hash cannot.  **C.** A secure hash produces a variable output for any input size; a secure cipher does not.  **D.** A secure cipher produces the same size output for any input size; a hash does not. |
|  | 118. | Which certificate format is typically used on Windows OS machines to import and export certificates and private keys?  **A.** DER **B.** AES **C.** PEM **D.** PFX |
|  | 119. | What is another name for an ephemeral key?  **A.** PKI private key **B.** MD5  **C.** PKI public key **D.** Session key |
|  | 120. | Why would a threat actor use steganography?  **A.** To test integrity **B.** To conceal information  **C.** To encrypt information **D.** To create a hashing value |
|  | 121. | The CIO has instructed you to set up a system where credit card data will be encrypted with the most secure symmetric algorithm with the least amount of CPU usage. Which of the following algorithms would you choose?  **A.** AES **B.** SHA-1 **C.** MD5 **D.** 3DES |
|  | 122. | Which of the following encryption methods is used by RADIUS?  **A.** Asymmetric **B.** Symmetric **C.** Elliptic curve **D.** RSA |
|  | 123. | When setting up a secure wireless company network, which of the following should you avoid?  **A.** WPA **B.** WPA2 **C.** EAP-TLS **D.** PEAP |
|  | 124. | You want to authenticate and log connections from wireless users connecting with EAP-TLS. Which of the following should be used?  **A.** Kerberos **B.** LDAP **C.** SAML **D.** RADIUS |
|  | 125. | Which of the following would be used to allow certain traffic to traverse from a wireless network to an internal network?  **A.** WPA **B.** WEP **C.** Load balancers **D.** 802.1x |
|  | 126. | You are asked to see if several confidential files have changed, and you decide to use an algorithm to create message digests for the confidential files. Which algorithm would you use?  **A.** AES **B.** RC4 **C.** Blowfish **D.** SHA-1 |
|  | 127. | Network data needs to be encrypted, and you are required to select a cipher that will encrypt 128 bits at a time before the data are sent across the network. Which of the following would you choose?  **A.** Stream cipher **B.** Hash algorithm  **C.** Block cipher **D.** Obfuscation |
|  | 128. | Which of the following are considered cryptographic hash functions? (Choose two.)  **A.** AES **B.** MD5 **C.** RC4 **D.** SHA-256 |
|  | 129. | A company’s database is beginning to grow, and the data-at-rest are becoming a concern with the security administrator. Which of the following is an option to secure the data-at-rest?  **A.** SSL certificate **B.** Encryption  **C.** Hashing **D.** TLS certificate |
|  | 130. | Which of the following hardware devices can store keys? (Choose two.) **A.** USB flash drive **B.** Smartcard  **C.** PCI expansion card **D.** Cipher lock |
|  | 131. | You are a security manager and have been asked to encrypt database system information that contains employee social security numbers. You are looking for an encryption standard that is fast and secure. Which of the following would you suggest to accomplish the requirements?  **A.** SHA-256 **B.** AES **C.** RSA **D.** MD5 |
|  | 132. | James is a security administrator and wants to ensure the validity of public trusted certificates used by the company’s web server, even if there is an Internet outage. Which of the following should James implement?  **A.** Key escrow **B.** Recovery agent **C.** OCSP **D.** CSR |
|  | 133. | You are a security administrator looking to implement a two-way trust model. Which of the following would you use?  **A.** ROT13 **B.** PGP **C.** WPA2 **D.** PKI |
|  | 134. | If a threat actor obtains an SSL private key, what type of attack can be performed? (Choose two.)  **A.** Eavesdropping **B.** Man-in-the-middle  **C.** Social engineering **D.** Brute force |
|  | 135. | Most authentication systems make use of a one-way encryption process. Which of the following is an example of a one-way encryption?  **A.** Symmetric algorithm **B.** Hashing Ch  **C.** Asymmetric algorithm **D.** PKI |
|  | 136. | 136. Which of the following transpires in a PKI environment?  **A.** The CA signs the certificate.  **B.** The RA signs the certificate.  **C.** The RA creates the certificate and the CA signs it.  **D.** The CA creates the certificate and the RA signs it. |
|  | 137. | Which of the following statements best describes how a digital signature is created?  **A.** The sender encrypts a message digest with the receiver’s public key. **B.** The sender encrypts a message digest with the receiver’s private key. **C.** The sender encrypts a message digest with his or her private key.  **D.** The sender encrypts a message digest with his or her public key. |
|  | 138. | AES is an algorithm used for which of the following?  **A.** Encrypting a large amount of data  **B.** Encrypting a small amount of data  **C.** Key recovery  **D.** Key revocation |
|  | 139. | PEAP protects authentication transfers by implementing which of the following?  **A.** TLS tunnels **B.** SSL tunnels  **C.** AES **D.** SHA hashes |
|  | 140. | AES-CCMP uses a 128-bit temporal key and encrypts data in what block size?  **A.** 256 **B.** 192 **C.** 128 **D.** 64 |
|  | 141. | Which of the following implement Message Integrity Code (MIC)? (Choose two.)  **A.** AES **B.** DES **C.** CCMP **D.** TKIP |
|  | 142. | James, a WLAN security engineer, recommends to management that WPA-Personal security should not be deployed within the company’s WLAN for their vendors. Which of the following statements best describe James’s recommendation? (Choose two.)  **A.** Static preshared passphrases are susceptible to social engineering attacks.  **B.** WPA-Personal uses public key encryption.  **C.** WPA-Personal uses a weak TKIP encryption.  **D.** WPA-Personal uses a RADIUS authentication server. |
|  | 143. | Which of the following is correct regarding root certificates?  **A.** Root certificates never expire.  **B.** A root certificate contains the public key of the CA.  **C.** A root certificate contains information about the user.  **D.** A root certificate cannot be used to authorize subordinate CAs to issue certificates on its behalf. |
|  | 144. | Which of the following statements are correct about public and private key pairs? (Choose two.)  **A.** Public and private keys work in isolation of each other.  **B.** Public and private keys work in conjunction with each other as a team.  **C.** If the public key encrypts the data using an asymmetric encryption algorithm, the corresponding private key is used to decrypt the data.  **D.** If the private key encrypts the data using an asymmetric encryption algorithm, the receiver uses the same private key to decrypt the data. |
|  | 145. | Which of the following are the filename extensions for PKCS #12 files? (Choose two.)  **A.** .p12 **B.** .KEY **C.** .pfx **D.** .p7b |
|  | 146. | Your company has discovered that several confidential messages have been intercepted. You decide to implement a web of trust to encrypt the files. Which of the following are used in a web of trust concept? (Choose two.)  **A.** RC4 **B.** AES **C.** PGP **D.** GPG |
|  | 147. | Which of the following algorithms is typically used to encrypt data-at-rest?  **A.** Symmetric **B.** Asymmetric  **C.** Stream **D.** Hashing |
|  | 148. | Which of the following can assist in the workload of the CA by performing identification and authentication of users requesting certificates?  **A.** Root CA **B.** Intermediate CA  **C.** Registered authority **D.** OSCP |
|  | 149. | You recently upgraded your wireless network so that your devices will use the 802.11n protocol. You want to ensure all communication on the wireless network is secure with the strongest encryption. Which of the following is the best choice?  **A.** WEP **B.** WPA **C.** WPA2 **D.** WPS |
|  | 150. | A college wants to move data to a USB flash drive and has asked you to suggest a way to secure the data in a quick manner. Which of the following would you suggest?  **A.** 3DES **B.** SHA-256 **C.** AES-256 **D.** SHA-512 |