

Management 414: SANS CISSP® 10 Domains +S QUIZ -- Domain 5

1. Which of the following is a cipher that uses one particular letter to replace another?
 - a) Polyalphabetic cipher
 - b) Monoalphabetic cipher
 - c) Caesar cipher
 - d) Polymorphic cipher
2. Which of the following plays the MOST important part in protecting a cryptosystem?
 - a) A sufficiently large key length
 - b) Using a newer cipher such as Rijndael or Blowfish, versus an older cipher like 3DES
 - c) Protecting the secret key for a symmetric cryptosystem and the private key for a public-key cryptosystem
 - d) Ensuring the cipher used has been publicly studied and scrutinized for errors
3. Which of the following BEST describes non-repudiation as it relates to a cryptosystem?
 - a) The cryptosystem should be able to prove that the message has not been tampered with.
 - b) The cryptosystem should allow a person to know for sure that the message given to him by another person is really from that person.
 - c) The cryptosystem should hide the contents of the message from all other persons except the sender and the intended recipient.
 - d) The cryptosystem should be able to prove that a specific person, and only that person, sent the message and that it has not been altered or falsified.
4. Which of the following BEST describes the ROT-13 cipher?
 - a) It rotates each letter in the message thirteen places through the alphabet.
 - b) It runs the message through the Rijndael cipher thirteen successive times.
 - c) It runs the message through the ROT-3 cipher thirteen successive times.
 - d) It applies the Caesar cipher thirteen times to the message.
5. With respect to block cipher algorithms, CBC stands for which of the following?
 - a) Cipher Block Chaining
 - b) Code Book Cipher
 - c) Cipher Block Code
 - d) Code Block Chain
6. Which of the following is NOT a symmetric-key cryptosystem?
 - a) RC4
 - b) RSA
 - c) IDEA
 - d) DES

Management 414: SANS CISSP® 10 Domains +S QUIZ - Domain 5

7. Which of the following is NOT a characteristic of public-key cryptosystems?
 - a) Public-key cryptosystems are "slower" than symmetric-key cryptosystems when encrypting and decrypting a message.
 - b) Public-key cryptosystems distribute public-keys within digital signatures.
 - c) Public-key cryptosystems require a secure key distribution channel.
 - d) Public-key cryptosystems provide technical non-repudiation via digital signatures.
8. Hash functions provide what primary function in a cryptosystem?
 - a) Confidentiality
 - b) Non-repudiation
 - c) Authentication
 - d) Message integrity
9. Which of the following is NOT a hash function algorithm?
 - a) SHA
 - b) ECC
 - c) MD5
 - d) HMAC
10. Which of following does NOT provide for confidentiality?
 - a) CAST
 - b) IDEA
 - c) 3DES
 - d) MD5
11. Kerberos' main application is which of the following?
 - a) A public-key cryptosystem used in Microsoft products
 - b) A single sign-on system for client-server authentication schemes
 - c) A hash function used for integrity in modern cryptosystems
 - d) An authentication scheme used with TLS (Transaction Layer Security)
12. Double-DES, or 2DES, is not considered much stronger than DES for which of the following reasons?
 - a) Double-DES is vulnerable to the meet-in-the-middle attack.
 - b) Double-DES has an effective key length of 47 bits due to the double encryption of the message.
 - c) Because DES is not a mathematical "group", successive iterations of message encryption produce weaker and weaker ciphertext with respect to cryptanalysis.
 - d) Each successive pass of encryption using DES reduces the effective key length by 9 bits.

Management 414: SANS CISSP® 10 Domains +S QUIZ - Domain 5

13. The AES (Advanced Encryption Standard) uses which of the following algorithms?
 - a) Serpent
 - b) Twofish
 - c) Blowfish
 - d) Rijndael
14. The RSA algorithm uses what kind of intractable problem as the basis of its cryptosystem?
 - a) Solving the discrete logarithm problem over finite fields
 - b) Computing elliptic curves over finite fields
 - c) Factoring super-polynomials
 - d) Factoring certain large integers into their two prime factors
15. Which of the following key issues is based on the fact that the keys are not going to last forever, but if you do not discard it someone else may be able to use it?
 - a) Key theft
 - b) Key generation
 - c) Key change
 - d) Key retirement
16. Chosen ciphertext attacks are mainly used against which kind of ciphers?
 - a) Private-key
 - b) Symmetric-key
 - c) Public-key
 - d) Hash functions
17. Which of the following is one of the main differences between cryptography and steganography?
 - a) Cryptography provides secrecy but not confidentiality, whereas steganography provides confidentiality but does not provide secrecy (unless combined with cryptography).
 - b) Cryptography and steganography both provide secrecy, but only steganography provides confidentiality.
 - c) Steganography uses cryptography to provide secrecy.
 - d) Cryptography provides confidentiality but not secrecy, whereas steganography provides secrecy but does not provide confidentiality (unless combined with cryptography).
18. Which of the following is NOT a steganography method?
 - a) Superimposition
 - b) Injection
 - c) Substitution
 - d) Generation of a new file

Management 414: SANS CISSP® 10 Domains +5 QUIZ - Domain 5

19. Which of the following is also referred to as rotor systems, such as the 'American sigaba'?
- a) Hebern machines
 - b) Enigma machines
 - c) Vernam ciphers
 - d) Jefferson disks
20. What is the 'weakest link' in cryptographic systems?
- a) The key length of the cipher
 - b) The particular cipher, such as 3DES or Blowfish
 - c) The number of rounds of encryption, such as three for 3DES and one for DES
 - d) Protection and secure storage of public/private and symmetric keys
21. Which of the following is NOT a method of encryption?
- a) Substitution
 - b) Combination
 - c) Permutation
 - d) Hybrid
22. Which type of cryptosystem uses a one-way transformation and does not perform key-based encryption?
- a) Symmetric encryption functions
 - b) Asymmetric cryptographic functions
 - c) Diffie-Hellman exchange functions
 - d) Hash functions
23. Which algorithms are used for message integrity?
- a) MD5 and SHA-1
 - b) RSA and RC4
 - c) DES and 3DES
 - d) Diffie-Hellman and DSS
24. What is an adaptive-chosen plaintext attack?
- a) An adaptive-chosen plaintext attack allows the cryptanalyst to choose the initial ciphertext that gets decrypted, and then choose additional blocks of text that get decrypted for further analysis based upon each decryption step.
 - b) An adaptive-chosen plaintext attack allows the cryptanalyst to choose the initial plaintext that gets encrypted, and then choose additional blocks of text that get decrypted for further analysis based upon each decryption step.
 - c) An adaptive-chosen plaintext attack allows the cryptanalyst to choose the initial plaintext that gets encrypted, and then choose additional blocks of

Management 414: SANS CISSP® 10 Domains +S QUIZ-Domain 5

text that get encrypted for further analysis based upon each encryption step, d) An adaptive-chosen plaintext attack allows the cryptanalyst to choose the initial ciphertext that gets decrypted, and then choose additional blocks of text that get encrypted for further analysis based upon each encryption step.

25. Which component of IPSec provides encryption and limited authentication?

- a) AH (Authentication Header)
- b) ESP (Encapsulation Security Payload)
- c) SA (Security Association)
- d) VPN (Virtual Private Network)

26. The U.S. Government's clipper chip embodied the escrowed encryption standard using which of the following algorithms?

- a) Blowfish
- b) RC4
- c) Skipjack
- d) 3DES

27. What does AES stand for?

- a) Advanced Encryption Sample
- b) Advanced Encryption Sanction
- c) Advanced Encryption Signal
- d) Advanced Encryption Standard

28. Which of the following requirements is NOT a goal of cryptography?

- a) Confidentiality
- b) Availability
- c) Non-repudiation
- d) Authentication

29. Which of the following choices is NOT one of the four common cryptographic terms?

- a) Ciphertext
- b) Plaintext
- c) Decryption
- d) Authentication

Management 414: SANS CISSP® 10 Domains +S QUIZ - Domain 5

30. Given the following plaintext and cipher text, which choice would be the encryption for the word CAB?
1. Plaintext: A B C D E F
 2. Ciphertext: W K M P D O
- a) MDK
 - b) MKW
 - c) MWK
 - d) WKM
31. Using the ROT-3 scheme, which of the following choices would be the correct encryption for the word CAB?
- a) ABC
 - b) EFG
 - c) BAC
 - d) FDE
32. Which of the following choices describes the basic encryption technique of shuffling the order in which the characters appear?
- a) Permutation
 - b) Rotation
 - c) Hybrid
 - d) Substituting
33. Block ciphers can operate in several modes. Which of the following modes is the simplest, most obvious application?
- a) Electronic Codebook (ECB)
 - b) Output Feedback (OFB)
 - c) Cipher Feedback (CFB)
 - d) Cipher Block Chaining (CBC)
34. Block ciphers can operate in several modes. Which of the following modes is susceptible to a variety of brute-force attacks?
- a) Output Feedback (OFB)
 - b) Electronic Codebook (ECB)
 - c) Cipher Feedback (CFB)
 - d) Cipher Block Chaining (CBC)
35. There are three general types of crypto algorithms. Which of the following algorithms offers no key encryption?
- a) Symmetric
 - b) Asymmetric
 - c) Secret key
 - d) Hash

Management 414: SANS CISSP® 10 Domains +S QUIZ - Domain 5

36. Which of the following crypto attacks requires only encrypted messages (no plaintext is available)?
- a) Chosen-key attack
 - b) Chosen-ciphertext attack
 - c) Ciphertext-only attack