

## Post-Class Quiz: Cryptography Domain

---

1. Which of the following is not an objective of cryptography?
  - A. Confidentiality
  - B. Integrity
  - C. Availability
  - D. Non-repudiation
  
2. Who first invented wheel cipher?
  - A. The Greeks
  - B. Julius Caesar
  - C. Thomas Jefferson
  - D. Charles Babbage
  
3. An act to convert plaintext into ciphertext in order to preserve confidentiality of data is called?
  - A. Encryption
  - B. Decryption
  - C. Hash
  - D. Message authentication
  
4. A cipher that scrambles letters into different positions is referred to as what?
  - A. Substitution
  - B. Stream
  - C. Running key
  - D. Transposition
  
5. Which of the following is not a block cipher mode of operation in stream mode?
  - A. Electronic Code Book (ECB)
  - B. Cipher Feed Back (CFB)
  - C. Output Feed Back (OFB)
  - D. Counter (CTR)
  
6. What is a mathematical encryption operation that cannot be reversed called?
  - A. DES

## Post-Class Quiz: Cryptography Domain

---

- B. Transposition
  - C. Substitution
  - D. One-way hash
7. In block cipher, what creates the element of diffusion?
- A. Permutation using a lookup table
  - B. Bit substituting using a S-box
  - C. Use of a Feistel network
  - D. Use of a key scheduler
8. What is the effective key length for Data Encryption Standard (DES)?
- A. 56-bit
  - B. 64-bit
  - C. 32-bit
  - D. 16-bit
9. Data Encryption Standard (DES) performs how many rounds of permutation and substitution?
- A. 16
  - B. 32
  - C. 64
  - D. 56
10. Which of the following statements is not true?
- A. TDES has a mode that uses 2 keys
  - B. TDES has a mode that uses 3 keys
  - C. TDES offers a greater protection over DES
  - D. TDES has a mode that uses 1 key
11. Which of the following identifies the encryption algorithm selected by NIST for the new Advanced Encryption Standard (AES)?
- A. RC6
  - B. Serpent

- C. Rijndael
  - D. Twofish
12. Who vouches for the binding between the data items in a digital certificate?
- A. Issuing authority
  - B. Vouching authority
  - C. Certificate authority (CA)
  - D. Registration authority
13. What is the primary role of smartcards in a PKI?
- A. Transparent renewal of user keys
  - B. Fast hardware encryption of the raw data
  - C. Tamperproof, mobile storage and application of private keys of the users
  - D. Easy distribution of the certificates between the users
14. Which protocol makes use of an electronic wallet on a customer's PC and sends encrypted credit card information to merchant's Web server, which digitally signs it and sends it on to its processing bank?
- A. SSH
  - B. SSL
  - C. S/MIME
  - D. SET
15. Which of the following keys has the shortest lifespan?
- A. Private key
  - B. Session key
  - C. Public key
  - D. Secret key
16. Which of the following statements is most accurate of digital signature?
- A. It allows the recipient of data to prove the source and integrity of data.
  - B. It can be used as a signature system and a cryptosystem.
  - C. It is a method used to encrypt confidential data.

## Post-Class Quiz: Cryptography Domain

---

- D. It is the art of transferring handwritten signature to electronic media.
17. Which of the following mail standards relies on a "Web of Trust"?
- A. Pretty Good Privacy (PGP)
  - B. Privacy Enhanced Mail (PEM)
  - C. MIME Object Security Services (MOSS)
  - D. Secure Multipurpose Internet Mail Extensions (S/MIME)
18. Electronic signatures can prevent messages from being:
- A. Erased
  - B. Forwarded
  - C. Disclosed
  - D. Repudiated
19. Which of the following are suitable protocols for securing VPN connections?
- A. S/MIME and SSH
  - B. PKCS#10 and X.509
  - C. TLS and SSL
  - D. IPsec and L2TP
20. Which of the following techniques is used in the encryption of data between a web browser and server?
- A. PGP
  - B. IPsec
  - C. Kerberos
  - D. SSL
21. The Diffie-Hellman algorithm is primarily used to provide which of the following?
- A. Key exchange
  - B. Integrity
  - C. Non-repudiation
  - D. Confidentiality

## Post-Class Quiz: Cryptography Domain

---

22. Which of the following asymmetric encryption algorithms is based on the difficulty of factoring large numbers?
- A. International Data Encryption Algorithm (IDEA)
  - B. RSA
  - C. Elliptic Curve Cryptosystems (ECCs)
  - D. El Gamal
23. What can be defined as secret communications where the very existence of the message is hidden?
- A. Vernam cipher
  - B. Steganography
  - C. Cryptology
  - D. Clustering
24. What is the role of internet key exchange (IKE) within the IPsec protocol?
- A. enforcing quality of service
  - B. data signature
  - C. data encryption
  - D. peer authentication and key exchange
25. Which of the following should be used as a replacement for Telnet for secure remote login over an insecure network?
- A. S-Telnet
  - B. SSH
  - C. SSL
  - D. Rlogin
26. Which of the following statements is true about data encryption as a method of protecting data?
- A. It requires careful key management.
  - B. It should sometimes be used for password files.
  - C. It is usually easily administered.
  - D. It makes few demands on system resources.

## Post-Class Quiz: Cryptography Domain

---

27. Which type of attack is based on the probability of two different messages using the same hash function producing a common message digest?
- A. Statistical attack
  - B. Differential cryptanalysis
  - C. Differential linear cryptanalysis
  - D. Birthday attack
28. Which of the following encryption methods is unbreakable?
- A. DES codebooks
  - B. One-time pads
  - C. Elliptic-curve cryptography
  - D. Symmetric ciphers
29. Which of the following is not related to a Public key infrastructure (PKI)?
- A. A X.509 certificate
  - B. A Registration authority
  - C. A Ticket Granting Service
  - D. A Certificate authority
30. Why does a digital signature contain a message digest?
- A. To indicate the encryption algorithm
  - B. To confirm the identity of the sender
  - C. To enable transmission in a digital format
  - D. To detect any alteration of the message
31. The Clipper Chip utilizes which concept in public key cryptography?
- A. Key Escrow
  - B. Substitution
  - C. An undefined algorithm
  - D. Super strong encryption
32. The DES encryption scheme has which of the following pair of characteristics?
1. a secret key encryption algorithm

2. a public key encryption algorithm
  3. a symmetric key distribution system
  4. an asymmetric key distribution
    - A. 1 and 4
    - B. 1 and 3
    - C. 2 and 3
    - D. 2 and 4
33. Public Key algorithms are:
- A. Two times faster than secret key algorithms
  - B. Two times slower than secret key algorithms
  - C. 1,000 to 10,000 times slower than secret key algorithms
  - D. 1,000 to 10,000 times faster than secret key algorithms
34. Cryptography does not concern itself with:
- A. Availability
  - B. Authenticity
  - C. Integrity
  - D. Confidentiality
35. Which of the following is not a mode of the Data Encryption Standard (DES)?
- A. Electronic Code Book (ECB)
  - B. Output Feedback (OFB)
  - C. Substitution
  - D. Cipher Block Chaining (CBC)
36. Which of the following is not true about DES?
- A. It uses 16 rounds of transposition and substitution
  - B. It encrypts 64 bits of text at a time
  - C. It is an asymmetric cipher
  - D. It has 8 bits for parity in its key
37. What does AES use S-boxes for during the process of encryption?

## Post-Class Quiz: Cryptography Domain

---

- A. Substitution
  - B. Key generation
  - C. Key exchange
  - D. Chaining
38. Which of the following protects Kerberos against replay attacks?
- A. Passwords
  - B. Cryptography
  - C. Time stamps
  - D. Tokens
39. What is the result of a hash algorithm being applied to a message?
- A. A plaintext
  - B. A message digest
  - C. A ciphertext
  - D. A digital signature
40. A public key algorithm that does both encryption and digital signature is which of the following?
- A. RSA
  - B. DES
  - C. IDEA
  - D. DSS
41. In what way does the RSA algorithm differ from the Data Encryption Standard (DES)?
- A. It cannot produce a digital signature.
  - B. It eliminates the need for a key-distribution center.
  - C. It is based on a symmetric algorithm.
  - D. It uses a public key for encryption.
42. The RSA algorithm is an example of what type of cryptography?
- A. Private Key

## Post-Class Quiz: Cryptography Domain

---

- B. Secret Key
  - C. Symmetric key
  - D. Asymmetric key
43. What is the primary reason for using one-way hashing algorithms on user passwords?
- A. It provides the compression necessary to conserve hard disk space on the host system
  - B. It eliminates the excessive processing required of symmetric encryption.
  - C. It prevents people from seeing the passwords in clear text
  - D. It provides a simplified platform for password for most password cracking utilities
44. A person in possession of a sample of the ciphertext and the corresponding plaintext is capable of what type of attack?
- A. Known-plaintext
  - B. Ciphertext only
  - C. Chosen-plaintext
  - D. Plaintext
45. What does S/MIME do?
- A. It adds security to e-mail messages in MIME format
  - B. It offers the same functionality as PEM
  - C. It provides data security
  - D. It provides a secure channel for communication
46. Which of the following is not a good description of Pretty Good Privacy (PGP)?
- A. It uses a web of trust between the participants
  - B. It uses a hierarchical trust model
  - C. It was created by Phil Zimmerman
  - D. It uses passphrases
47. All of the following are hashing algorithms with the exception of?
- A. SHA

## Post-Class Quiz: Cryptography Domain

---

- B. IDEA
  - C. HAVAL
  - D. MD2
48. Which answer is not true of the Diffie-Hellman algorithm?
- A. IT Security stems from the difficulty of calculating the product of two large prime numbers
  - B. It was the first public key exchange algorithm
  - C. It is vulnerable to man-in-the-middle attacks
  - D. It is used for key distribution of a shared key, but not used for message encryption and decryption
49. Which is not an attribute of a one-way trap door?
- A. It is a mathematical function that is easier to compute in one direction than the opposite direction
  - B. The forward direction of a one-way function can take seconds to encrypt and the opposite direction can take years to figure out.
  - C. One-way function is used in symmetric key cryptography because they have to know about the trap door to decrypt
  - D. RSA is based on a trap door one-way function
50. Which is not true about fair cryptosystems?
- A. It splits the private key into different parts
  - B. It gives law enforcement access when legally authorized
  - C. It escrows the separate key parts with separate escrow agencies
  - D. It uses a tamper proof chip
51. Which answer does not describe a characteristic of the Clipper Chip?
- A. It uses the SkipJack algorithm
  - B. It uses a software-based escrow solution
  - C. It was developed by the NSA
  - D. It has an 80 bit key length
52. Which of the following is unbreakable by intensive search or brute force attacks?

## Post-Class Quiz: Cryptography Domain

---

- A. TDES
  - B. Steganography
  - C. IDEA
  - D. One-time pad
53. Data hidden in the slack space of a disk is called?
- A. Concealment cipher usage
  - B. Steganography
  - C. Transposition
  - D. Permutation
54. Of the following, which is most true?
- A. RSA gets its strength from the complexity of using discrete logarithms in a finite field
  - B. El Gamal gets its strength from the complexity of using discrete logarithms in a finite field
  - C. ECC gets its strength from the complexity of factoring the product of two large prime numbers
  - D. Diffie-Hellman gets its strength from the complexity of factoring the product of two large prime numbers
55. Which of the following statements is not true of symmetric key algorithms?
- A. They are slower than asymmetric algorithms
  - B. They provide key distribution problems
  - C. Keys need to be exchanged “out of band”
  - D. They do not provide authentication and non repudiation
56. Which single answer is not a symmetric key algorithm?
- A. RC4
  - B. Blowfish
  - C. DES
  - D. RSA
57. Which statement is the most accurate?

## Post-Class Quiz: Cryptography Domain

---

- A. HTTPS and SHTTP are the same thing
  - B. HTTPS is HTTP that is being used over SSL
  - C. SHTTP is SSL that is being used over HTTP
  - D. HTTPS is more robust and secure version of SHTTP
58. Which characteristic is not that of a good stream cipher?
- A. Long periods of no repeating patterns
  - B. Statistically predictable
  - C. Keystream is not linearly related to the key
  - D. Statistically unbiased keystream
59. What is the best description of a stream cipher?
- A. The message is divided into blocks and mathematical functions are performed on each block
  - B. The sender must encrypt the message with his/her private key so the receiver can decrypt it with her/his public key
  - C. The cipher uses a key to create a keystream and XOR's the result with the message
  - D. The cipher executes 16 rounds of computation on each bit?
60. Which best describes the process of a secure socket layer (SSL) connection?
- A. The server creates a session key and encrypts it with a private key
  - B. The server creates a session key and encrypts it with a public key
  - C. The client creates a session key and encrypts it with a private key
  - D. The client creates a session key and encrypts it with a public key
61. Of the following, which is the best description of a digital signature?
- A. The sender encrypts a message digest with his/her public key
  - B. The sender encrypts a message digest with his/her private key
  - C. The recipient encrypts a message digest with his/her public key
  - D. The recipient encrypts a message digest with his/her private key
62. What is a public key used for?

## Post-Class Quiz: Cryptography Domain

---

- A. It authenticates a network interface
  - B. It authenticates a covert channel
  - C. It authenticates a private key
  - D. It authenticates VPN connections
63. Which of the following is required for cryptanalysis?
- A. Access to the plain text
  - B. Access to the algorithm source
  - C. Access to the cipher text and algorithm source
  - D. Access to plain text and ciphertext
64. Which items is the responsibility of key management?
- A. Key generation and destruction
  - B. Access controls and encryption
  - C. Key length and algorithm propriety
  - D. Access control, user authentication and authorization
65. The HAVAL algorithms perform what function?
- A. Hashing
  - B. Key distribution
  - C. Digital signature
  - D. Encryption

## Post-Class Quiz: Cryptography Domain

---

66. What is the Clipper Chip key size?

- A. 80 bit
- B. 64 bit
- C. 128 bit
- D. 160 bit

67. What technology encrypts the header, trailer and routing information in the communications path?

- A. Data hiding
- B. Link encryption
- C. End-to-end encryption
- D. S/MIME