VIT Vidyalankar Institute of Technology
Accredited A+ by NAAC

IA-01 Online Examination, Vidyalankar Institute of Technology

Semester:	V
Subject :	Computer Network Security
Date of Examination:	30-08-2021
QB Prepared BY	Prof Vinita Bhandiwad & Prof Yash Shah

1. Which is not one of the security goals?
    a. Confidentiality
    b. Integrity
    c. Authentication
    d. Availability
2. Ceaser Cipher is type of
    a. Transposition Cipher
    b. Substitution Cipher
    c. Block Cipher
    d. Asymmetric key ciphers
3. The Value of Key in Ceaser Cipher is
    a. 4
    b. 5
    c. 3
    d. 7
4. If the received Cipher is Z and the value of key 15, what is the plain text if Additive cipher was used?
    a. A
    b. D
    c. L
    d. K
5. If the received Cipher is J, what is the plain text if Cesear Cipher was used?
    a. G
    b. B
    c. V
    d. W
6. Playfair is a
    a. Monoalphabetic Cipher
    b. Polyalphabetic Cipher
    c. Block Cipher
    d. Asymmetric key ciphers
7. Vigenere is a
    a. Monoalphabetic Cipher
    b. Polyalphabetic Cipher
    c. Block Cipher
    d. Asymmetric key ciphers
8. Affine Cipher is a combination of
    a. Additive and ceaser Cipher
    b. Additive and Multiplicative Cipher
    c. Ceaser and Multiplicative Cipher
    d. Playfair and Vigenere Cipher

9. Keyed columnar is a type of
    a. Transposition Cipher
    b. Substitution Cipher
    c. Block Cipher
    d. Asymmetric key ciphers
10. Calculate the Cipher for Plain text = 'hello everyone' and key = 'HACK' using Keyed (column) Cipher
    a. eeyxhorelenxlvox
    b. eeyxlovxhorelenx
    c. eeyxlovxlenxhore
    d. eeyxlenxlovxhore
11. Which is not a type of block cipher
    a. Data Encryption Standard (DES)
    b. Double DES
    c. Message digest 5
    d. Advanced Encryption Standard (AES)
12. Public key cryptography is also known as
    a. Transposition Cipher
    b. Substitution Cipher
    c. Block Cipher
    d. Asymmetric key ciphers
13. The DES Algorithm Cipher System consists of _____rounds (iterations) each with a round key
    a. 12
    b. 8
    c. 15
    d. 16
14. The DES algorithm has a key length of
    a. 128 Bits
    b. 32 Bits
    c. 64 Bits
    d. 16 Bits
15. In the DES algorithm, although the key size is 64 bits only 48bits are used for the encryption procedure
    a. True
    b. False
16. In the DES algorithm the 64 bit key input is shortened to 56 bits by ignoring every 4th bit.
    a. True
    b. False
17. DES Follows
    a. Hash Algorithm
    b. Caesars Cipher
    c. Feistel Cipher Structure
    d. SP Networks
18. How many rounds does the AES-192 perform?
    a. 10
    b. 16
    c. 12
    d. 14
19. How many rounds does the AES-256 perform?
    a. 10
    b. 16

c. 12
d. 14

20. The 4×4 byte matrices in the AES algorithm are called
    a. States
    b. Words
    c. Transitions
    d. Permutation
21. Which of the following step doesn't happen in AES
    a. Sub Bytes
    b. Shift Rows
    c. Initial Permutation
    d. Mix Columns
22. In Add Round Key step
    a. State is multiplied with the key
    b. State is modulo added with the key
    c. State is divided with the key
    d. State is subtracted with the key
23. The size of input of pain text in DES is
    a. 128 bits
    b. 64 bits
    c. 32 bits
    d. 160 bits
24. The size of input of pain text in 3DES is
    a. 128 bits
    b. 64 bits
    c. 32 bits
    d. 160 bits
25. The size of input of pain text in 2DES is
    a. 128 bits
    b. 64 bits
    c. 32 bits
    d. 160 bits
26. RSA is named after the researchers (_____) who proposed it.
    a. River, Shamir, Adleman
    b. Rivest, Shamus, Adleman
    c. Rivest, Shamir, Adleman
    d. Rivest, Shamir, Adlemar
27. RSA is a
    a. Transposition Cipher
    b. Substitution Cipher
    c. Block Cipher
    d. Asymmetric key ciphers
28. In the RSA algorithm, we select 2 random large values 'p' and 'q'. Which of the following is the property of 'p' and 'q'?
    a. p and q should be divisible by Φ(n)
    b. p and q should be co-prime
    c. p and q should be prime
    d. p/q should give no remainder
29. In RSA, Φ(n) = _____ in terms of p and q.
    a. (p)/(q)

b. (p)(q)
c. (p-1)(q-1)
d. (p+1)(q+1)

30. In RSA, we select a value 'e' such that it lies between 0 and Φ(n) and it is relatively prime to Φ(n).
    a. True
    b. False
31. For p = 11 and q = 19 and choose e=17. Apply RSA algorithm where message=5 and find the cipher text.
    a. 80
    b. 92
    c. 56
    d. 23
32. Perform encryption on the following PT using RSA and find the CT. p = 3; q = 11; M = 5 ,e=3.
    a. 28
    b. 26
    c. 18
    d. 12
33. n = 35; e = 5; C = 10. What is the plaintext (use RSA)
    a. 3
    b. 7
    c. 8
    d. 5
34. Which is one of the authentication functions
    a. Secure Hash Algorithm
    b. Message Authentication Code (MAC)
    c. Message Digest 5
    d. Advanced Encryption Algorithm
    e. Data Encryption Standard
35. The two steps of biometric authentication are
    a. Authorization, encryption
    b. Identification, Validation
    c. Authentication, recognition
    d. Authentication, Authorization
36. SHA-1 produces a hash value of
    a. 256 bits
    b. 160 bits
    c. 180 bits
    d. 128 bits
37. What is the number of round computation steps in the SHA-1 algorithm?
    a. 80
    b. 76
    c. 64
    d. 70
38. SHA stands for?
    a. Secret Hash Algorithm
    b. Secure Help Area
    c. Secure Hash Algorithm
    d. Safe Hash Area
39. The Block Chunk size used in SHA is
    a. 256 bits

b. 130 bits
c. 128 bits
d. 512 bits

40. The length of padding bits in SHA is_____(Consider X = Length of message)
    a. $\chi * 64 - X$
    b. $\chi * 512 - X$
    c. $\chi * 512 - 64 - X$
    d. $\chi * 512 - 128 - X$
41. Size of buffer in SHA is
    a. 128 bits
    b. 160 bits
    c. 256 bits
    d. 512 bits
42. Which is not a property of a hash function?
    a. Changes arbitrary length input into fixed length output.
    b. Compresses the length
    c. Irreversible Process
    d. More than one message can have same Hash Code.
43. MD-5 produces a hash value of
    a. 256 bits
    b. 160 bits
    c. 180 bits
    d. 128 bits
44. What is the number of round computation steps in the MD-5 algorithm?
    a. 80
    b. 76
    c. 64
    d. 70
45. Size of buffer in MD-5 is
    a. 128 bits
    b. 160 bits
    c. 256 bits
    d. 512 bits
46. Which is false for Digital certificate
    a. Establish relation between user and public key
    b. Issued by trusted party
    c. Used for achieving confidentiality
    d. Contains username and public key
47. HMAC is used
    a. Generating message authentication code
    b. Encrypting the data
    c. Achieving integrity
    d. Achieving Availability
    e. Contains username and public key
48. CMAC is used
    a. Generating message authentication code
    b. Encrypting the data
    c. Achieving integrity
    d. Achieving Availability

49. Which is not a property of a hashing
    a. Hashing changes an arbitrary length message to a fixed length message
    b. Hashing compresses the size of plain text
    c. Hashing is an irreversible process
    d. Hashing can be used for achieving confidentiality
50. RFID is a type of
    a. Static Token Authentication
    b. Dynamic Token Authentication
    c. Password Based Authentication
    d. Biometric Authentication

Subject Teacher