Techno India Batanagar
Computer Science and Engineering

Model Questions

Subject Name: Cryptography and Network Security **Subject Code:** CS801D

Multiple Choice Questions

1. Rail Fence Technique is an example of
   a) Substitution
   b) Transposition
   c) Product cipher
   d) Caesar cipher

2. SET is
   a) Electronic Payment System
   b) Security Protocol
   c) Credit card payment
   d) Internet Payment System

3. Public key encryption is advantageous over Symmetric key Cryptography because of
   a) Speed
   b) Space
   c) Key exchange
   d) Key length

4. The sub key length at each round of DES is_____
   a) 32
   b) 56
   c) 48
   d) 64

5. MAC is used to ensure
   a) Authentication
   b) Confidentiality
   c) Authentication and integrity
   d) Authentication and confidentiality

6. Total no. of messages used in SSL Handshake Protocol is
   a) 12
   b) 10
   c) 8
   d) 14

7. A worm _____ modify a program.
   a) Does not
   b) Does
   c) May or may not
   d) None of these

8. Differential Cryptanalysis can be mounted on
   a) DES encryption algorithm
   b) AES encryption algorithm
   c) RSA encryption algorithm
   d) Deffie-Hellman key exchange algorithm

9. Which one is the strong attack mechanism?
   a) Chosen plaintext attack
   b) Chosen cipher text
   c) Brute Force Attack
   d) Man in the middle attack

10. Message Digest length in SHA 1 is_____ bits.
   a) 128
   b) 160
   c) 64
   d) 54

11. Interception is an attack on
   a) Availability
   b) Confidentiality
   c) Integrity
   d) Authenticity

12. _____ prevents either sender or receiver from denying a transmitted message.
   a) Access Control
   b) Non repudiation
   c) Masquerade
   d) Integrity

13. IDEA uses ____keys.
   a) 3
   b) 4
   c) 5
   d) 2

14. A Macro virus is
    a) Platform dependent
    b) Platform independent
    c) Idle
    d) Hidden

15. Which one of the following is active attack?
    a) Masquerade
    b) Traffic analysis
    c) Eavesdropping
    d) Shoulder surfing

16. Which of the following is passive attack?
    a) Relay attack
    b) Masquerade
    c) Traffic analysis
    d) Denial of Service

17. A firewall that uses two TCP connections is
    a) Bastion
    b) Application gateway
    c) Circuit level gateway
    d) Packet filtering

18. IPsec services are available in _____ Layer.
    a) Application
    b) Data link
    c) Network
    d) Transport

19. Caesar cipher is an example of
    a) Substitution cipher
    b) Transposition cipher
    c) Substitution as well as transposition
    d) None of these

20. The Authentication Header (AH) , part of IPsec, provides which of the following security function?
    a) Source authentication
    b) Data Integrity
    c) Data confidentiality

d) Source authentication and data integrity

21. To verify a digital signature we need the
    a) Sender's Private key
    b) Sender's Public key
    c) Receiver's Private key
    d) Receiver's Public key

22. The secure socket layer provides
    a) Encryption of messages sent by both client and server
    b) Server authentication
    c) Optional client authentication
    d) All of these.

23. No. of keys used in Asymmetric key Cryptography is
    a) 10
    b) 02
    c) 04
    d) 01

24. Vigenere cipher is an example of
    a) Polyalphabetic cipher
    b) Caesar cipher
    c) Mono alphabetic cipher
    d) Product cipher

25. Firewall may be described as specified form of
    a) Router
    b) Bridge
    c) Operating system
    d) Architecture

26. Tool for implementing security policy may be called as
    a) Security process
    b) Security authentication
    c) Security gaps
    d) Security mechanism

27. In MD-5 the length of the message digest is
    a) 160
    b) 128
    c) 64
    d) 54

28. RC4 is an example of
    a) Hash algorithm
    b) Stream cipher
    c) Block cipher
    d) None of these

29. For confidentiality, data to be sent is
    a) Encrypted
    b) Decrypted
    c) Corrected
    d) Both (a) and (b)

30. A polymorphic virus undergoes
    a) Crossover
    b) Mutation
    c) Genetic processing
    d) None of these.

31. Key used in the symmetric key cryptography is
    a) Public key
    b) Private key
    c) Permanent key
    d) Session key

32. Chosen cipher text attack is based on
    a) Cryptanalysis
    b) Cryptography
    c) Encryption
    d) Decryption

33. Authentication service that can be used in windows platform is
    a) DES
    b) RSA
    c) MD5
    d) KERBEROS

34. A virus that cannot be detected by antivirus software is
    a) Parasitic
    b) Polymorphic
    c) Stealth
    d) Worm

35. An attack ok authenticity is
    a) Interruption
    b) Interception
    c) Fabrication
    d) Violation

36. The process of writing the text as rows and read it as columns is known as
    a) Vernam cipher
    b) Caesar cipher
    c) Transposition columnar cipher
    d) Homophonic substitution cipher

37. The principal of _____ ensures that only the sender and the intended recipients have access to the contents of message
    a) Confidentiality
    b) Authentication
    c) Integrity
    d) Access control

38. In IDEA key is of _____ bits.
    a) 128
    b) 64
    c) 256
    d) 512

39. RSA_____ be used for digital signature.
    a) Must no
    b) Cannot
    c) Can
    d) Should not

40. _____ is a message digest algorithm.
    a) DES
    b) IDEA
    c) MD5
    d) RSA

41. Biometric authentication works on the basis of
    a) Human characteristics
    b) Passwords
    c) Smart cards
    d) Pin

42. _____ forms the basis for the randomness of authentication token.
   a) Password
   b) Seed
   c) MD5
   d) RSA

43. In polyalphabetic cipher, the characters in plaintext have a relation with the characters in cipher text
   a) One to one
   b) One to many
   c) Many to one
   d) Many to many

44. _____ is based on the idea of hiding the relationship between the cipher text and the Key
   a) Diffusion
   b) Confusion
   c) Both (a) and (b)
   d) None of these

45. There are _____ encryption rounds in IDEA.
   a) 5
   b) 16
   c) 10
   d) 8

46. The main goal of _____ attack is to obtain unauthorized access to the information.
   a) Active
   b) Caesar
   c) Passive
   d) Brute force

47. _____ involves trying every possible key until a proper translation of cipher text into plain text is obtained.
   a) Man in the middle attack
   b) Chosen Plain text Attack
   c) Brute Force attack
   d) None of these

48. Encryption Algorithm is
   a) Mode of Cryptography
   b) Security approach of cryptography

c) Components of cryptography
d) All of the above

49. _____ operates on smaller unit of plain text.
a) Block cipher
b) Stream cipher
c) Rail fence
d) Both (a) and (b)

50. In_____ mode, the same plaintext value will always result in the same cipher text value.
a) Cipher Block Chaining
b) Cipher Feedback
c) Electronic code book
d) Output Feedback

51. Which cryptographic mode includes the use of Initial Vector?
a) Electronic Code book mode
b) Cipher Block Chaining mode
c) Cipher Feedback mode
d) Output Feedback mode

52. The DES process involves ____ number of rounds.
a) 8
b) 32
c) 12
d) 16

53. RC5 is a type of
a) Block Cipher
b) Plain cipher
c) Stream Cipher
d) Caesar cipher

54. In Digital Signature, there is _____ relationship between signature and message.
a) Many to one
b) One to many
c) Many to many
d) One to one

55. When a Hash function is used to provide message authentication, the hash function value is referred to as
a) Message digest
b) Message authentication code

c) Hashed based MAC
d) None of these

56. In _____ , the malicious code is installed on a personal computer or server misdirecting usersto fraudulent website.
a) Phishing scam
b) Pharming scam
c) Spoofing
d) Sniffing

57. This web threat is used to fake one's identity
a) Sniffing
b) Spoofing
c) Pharming
d) Phishing

58. Which security protocol is used to secure pages where users are required to submit sensitive information?
a) Secure Socket Layer
b) Transport Layer Security
c) Secure IP
d) Secure HTTP

59. The criteria which makes TLS more secure than SSL is
a) Message Authentication
b) Key material generation
c) Both (a) and (b)
d) None of these

60. The _____ mode of IPsec, take the whole IP packet to form secure communication between two gateways
a) Transport
b) Tunnel
c) Either (a) or (b)
d) Both (a) and (b)

61. The _____ authentication factor that relate to something that a user is or does and includes biometric identifiers.
a) Knowledge factor
b) Ownership factor
c) Inherence Factor
d) Authentication factor

62. In password selection strategy, minimum length of characters used
    a) 6
    b) 10
    c) 8
    d) 14

63. Example of an Authentication Token is
    a) Key fob
    b) Smart card
    c) Pin
    d) None of these

64. A _____ acts as a barrier between a trusted network and an untrusted network
    a) Bridge
    b) Router
    c) Firewall
    d) Both (a) and (b)

65. It monitors the TCP handshaking going on between the local and remote host to determine whether the session being initiated is legitimate.
    a) Application Layer Firewall
    b) State full firewall
    c) Packet firewall
    d) Circuit level firewall

66. A substitution cipher substitutes one symbol with
    a) Keys
    b) Multi parties
    c) Single party
    d) Others

67. Man in the middle attack can endanger the security of Diffie Hellman method if two parties are not
    a) Joined
    b) Authenticated
    c) Submitted
    d) Shared

68. Which layer filters the proxy firewall?
    a) Application
    b) Network
    c) Transport
    d) None of the above

69. Hash function is used to produce
    a) Fingerprint of a file
    b) Useful for message authentication
    c) Both (a) and (b)
    d) None of the above

70. Name the network attack that floods it with useless traffic.
    a) Spoofing
    b) Denial of Service attack
    c) Virus
    d) Trojan Horse

71. Encryption Strength is based on
    a) Strength of Algorithm
    b) Secrecy of key
    c) Length of key
    d) All of the above

72. Kerberos is an authentication scheme that can be used for
    a) Public key cryptography
    b) Digital signature
    c) Hash function
    d) Single sign on

73. Which of the following is not a block cipher operating mode?
    a) ECB
    b) CFB
    c) CBF
    d) CBC

74. One Time Pad is also known as
    a) Playfair cipher
    b) Hill cipher
    c) Vigenere Cipher
    d) Perfect Secrecy

75. _____ is the name for Public Key Infrastructure certificate
    a) Man in the Middle attack
    b) Certificate Authority
    c) Resource Access Control facility

d) Script kiddy

76. Network Address Translation is_____ with transport mode.
   a) Supported
   b) Not supported
   c) May or may not supported
   d) Does not have any relation

77. Which one of the following belongs to SSL protocol?
   a) Handshake Protocol
   b) Change Cipher Spec protocol
   c) Both (a) and (b)
   d) None of the above

78. Encapsulating Security Payload (ESP) belongs to which Internet Security Protocol?
   a) Secure Socket Layer Protocol
   b) Secure IP Protocol
   c) Secure Http Protocol
   d) Transport Layer Security Protocol

79. The four Primary Security Principles related to messages are
   a) Confidentiality, Integrity, Non repudiation and Authentication.
   b) Confidentiality, Access Control, Integrity, Non repudiation.
   c) Authentication, Authorization, Availability, Integrity
   d) Availability, Authorization, Confidentiality, Integrity.

Answers to the Questions

1.(a) Transposition

2.(a) Electronic Payment System

3.(c) Key Exchange

4.(b) 56

5.(a) Authentication

6.(a) 12

7.(a) Does not

8.(a) DES encryption algorithm

9.(c) Brute Force Attack

10.(b) 160

11.(b) Confidentiality

12.(b) Non Repudiation

13.(b) 4

14.(b) Platform Independent

15.(a) Masquerade

16.(c) Traffic Analysis

17.(d) Packet Filtering

18.(c) Network

19.(a) Substitution cipher

20.(d) Source Authentication and data integrity

21.(b) Sender's Public key

22.(a) Encryption of messages both sent by client and Server

23.(b) 02

24.(a) Poly alphabetic Cipher

25.(a) Router

26.(d) Security Mechanism

27.(b) 128

28.(c) Block cipher

29.(a) Encrypted

30.(b) Mutation

31.(a) Public Key

32.(a) Cryptanalysis

33.(d) Kerberos

34.(c) Stealth

35.(b) Interception

36.(c) Transposition Columnar cipher

37.(b) Authentication

38.(a) 128

39.(c) Can

40.(c) MD5

41.(a) Human Characteristics

42.(a) Password

43.(b) One to Many

44.(b) Confusion

45.(d) 8

46.(c) Passive

47.(c) Brute Force Attack

48.(c) Component of Cryptography

49.(b) Stream Cipher

50.(c) Electronic codebook

51.(b) Cipher Block Chaining mode

52.(d) 16

53.(a) Block Cipher

54.(d) One to One

55.(a) Message Digest

56.(b) Pharming Scam

57.(b) Spoofing

58.(a) Secure Socket Layer

59.(c) both (a) and (b)

60.(b) Tunnel

61.(c) Inherence Factor

62.(c) 8

63.(b) Smart Card

64.(c) Firewall

65.(d) Circuit Level gateways protocol

66.(d) others

67.(b) Authenticated

68.(a) Application

69.(b) Useful for message authentication

70.(a) spoofing

71.(d) All of the above

72.(b) Digital Signature

73.(c) CBF

74.(d) Perfect Secrecy

75.(b) Certificate Authority

76.(b) not supported

77.(c) both (a) and (c)

78.(b) Secure IP Protocol

79.(a) Confidentiality, Integrity, Non repudiation, Authenticity