Dr.G.R.Damodaran College of Science

(Autonomous, affiliated to the Bharathiar University, recognized by the UGC)Re-accredited at the 'A' Grade Level by the **NAAC** and ISO 9001:2008 Certified
CRISL rated 'A' (TN) for MBA and MIB Programmes

IIII BSC (IT) [2015-2018]
Semester-V
ELECTIVE-I: CYBER SECURITY - 512U7
Multiple Choice Questions.

1. The size and complexity of networks grew enormously when:
   A. Only governments and universities owned computers
   B. Only governments and universities owned computers
   C. The number of personal computers greatly increased
   D. The hacktivists started using the internet
   ANSWER: C

2. Which of these groups exploits cyber vulnerabilities?
   A. Criminals
   B. Governments
   C. Hacktivists
   D. All of the above
   ANSWER: D

3. What is a computer network?
   A. A super computer owned only by the government
   B. A web of connected computers or devices
   C. A computer vulnerability
   D. An Internet service provider
   ANSWER: B

4. Why are cyber vulnerabilities unlikely to ever go away?
   A. They are side effects of the freedom and ease of communicating online
   B. They are protected in a secret base on the moon.
   C. The government wonot allow people to fix them.
   D. Criminals need them to steal identities.
   ANSWER: A

5. According to The Secret Lives of Hackers, what is hacking?
   A. Problem solving by using an objects properties in unexpected ways.
   B. Creating problems where there previously were none.
   C. Using materials as they were intended to be used to solve problems.
   D. All of the above
   ANSWER: A

6. Codes have been used for thousands of years in order to:
   A. Figure out where the enemy submarines are

B. Communicate with some but not others
C. Become a king
D. Send encrypted text messages
ANSWER: B

7. Which of these is regularly used for secure online communication?
A. Caesar cipher
B. Public-key cryptography
C. More Code
D. Morse code Enigma code
ANSWER: B

8. Which of the following is true regarding access lists applied to an interface?
A. You can place as many access lists as you want on any interface until you run out of memory.
B. You can apply only one access list on any interface.
C. One access list may be configured, per direction, for each layer 3 protocol configured on an interface.
D. You can apply two access lists to any interface.
ANSWER: C

9. What router command allows you to determine whether an IP access list is enabled on a particular interface?
A. show ip port
B. show access-lists
C. show ip interface
D. show access-lists interface
ANSWER: C

10. The first computer virus is --------
A. I Love You
B. Blaster
C. Sasser
D. Creeper
ANSWER: D

11. MCAfee is an example of
A. Photo Editing Software
B. Quick Heal
C. Virus
D. Antivirus
ANSWER: D

12. Which of the following is known as Malicious software?
A. illegalware
B. badware
C. malware
D. maliciousware
ANSWER: C

13. To protect a computer from virus, you should install -------- in your computer.
A. backup wizard
B. disk cleanup

C. antivirus
D. disk defragmenter
ANSWER: C

14. VIRUS stands for
A. Very Intelligent Result Until Source
B. Very Interchanged Resource Under Search
C. Vital Information Resource Under Slege
D. Viral Important Record User Searched
ANSWER: C

15. Which of the following is/are threats for electronic payment systems?
A. Computer worms
B. Computer virus
C. Trojan horse
D. All of the above
ANSWER: D

16. Key logger is a
A. Firmware
B. Antivirus
C. Spyware
D. All of the above
ANSWER: C

17. To protect yourself from computer hacker, you should turn on a
A. Script
B. Firewall
C. VLC
D. Antivirus
ANSWER: B

18. Firewalls are used to protect against --------
A. data driven attacks
B. fire attacks
C. virus attacks
D. unauthorised access
ANSWER: D

19. Which of the following describes programs that can run independently travel from system to system and disrupt computer communication? \
A. Viruses
B. Trojans
C. Droppers
D. Worm
ANSWER: D

20. When a logic bomb is activated by a time related event, it is known as -------
A. virus
B. trojan horse
C. time related bomb sequence

D. time bomb
ANSWER: D

21. In cryptography, what is cipher?
A. algorithm for performing encryption and decryption
B. encrypted message
C. both (a) and (b)
D. none of the mentioned
ANSWER: A

22. In asymmetric key cryptography, the private key is kept by
A. sender
B. receiver
C. sender and receiver
D. all the connected devices to the network
ANSWER: B

23. Which one of the following algorithm is not used in asymmetric-key cryptography?
A. rsa algorithm
B. diffie-hellman algorithm
C. electronic code book algorithm
D. none of the mentioned
ANSWER: C

24. What is data encryption standard (DES)?
A. block cipher
B. stream cipher
C. bit cipher
D. none of the mentioned
ANSWER: A

25. Cryptanalysis is used
A. to find some insecurity in a cryptographic scheme
B. to increase the speed
C. to encrypt the data
D. none of the mentioned
ANSWER: A

26. Which one of the following is a cryptographic protocol used to secure HTTP connection?
A. stream control transmission protocol (SCTP)
B. transport layer security (TSL)
C. explicit congestion notification (ECN)
D. resource reservation protocol
ANSWER: B

27. ElGamal encryption system is
A. symmetric key encryption algorithm
B. asymmetric key encryption algorithm
C. not an encryption algorithm
D. none of the mentioned
ANSWER: B

28. An asymmetric-key (or public-key) cipher uses
A. 1 Key
B. 2 Key
C. 3 Key
D. 4 Key
ANSWER: B

29. Man-in-the-middle attack can endanger security of Diffie-Hellman method if two parties are not
A. Authenticated
B. Joined
C. Submit
D. Separate
ANSWER: A

30. Shift cipher is sometimes referred to as the
A. Caesar cipher
B. Shift cipher
C. cipher
D. cipher text
ANSWER: A

31. Advanced Encryption Standard (AES), has three different configurations with respect to number of rounds and
A. Data Size
B. Round Size
C. Key Size
D. Encryption Size
ANSWER: C

32. In Cryptography, input bits are rotated to right or left in
A. Rotation Cipher
B. XOR cipher
C. cipher
D. cipher text
ANSWER: A

33. In Asymmetric-Key Cryptography, although RSA can be used to encrypt and decrypt actual messages, it is very slow if message is
A. Short
B. Long
C. Flat
D. Thin
ANSWER: B

34. The entire hostname has a maximum of
A. 255 characters
B. 127 characters
C. 63 characters
D. 31 characters
ANSWER: A

35. Domain Name System (DNS), can be pictured as an inverted hierarchical tree structure with one root node at top and a maximum of
A. 128 Levels
B. 129 Levels
C. 130 Levels
D. 131 Levels
ANSWER: A

36. Name of domain is domain name of node at top of the
A. Sub Tree
B. Main Tree
C. Last Tree
D. Bottom Tree
ANSWER: A

37. Domain, which is used to map an address to a name is called
A. Generic Domains
B. Inverse Domain
C. Small Domains
D. Sub-Domains
ANSWER: B

38. DNS client adds suffix atc.jhda.edu. before passing address to the
A. DNS Host
B. DNS Server
C. DNS Label
D. DNS Recipient
ANSWER: B

39. Wildcard domain names start with label
A. @
B. *
C. &
D. #
ANSWER: B

40. The domain name system is maintained by
A. distributed database system
B. a single server
C. a single computer
D. none of the mentioned
ANSWER: A

41. IPSec is designed to provide the security at the
A. transport layer
B. network layer
C. application layer
D. session layer
ANSWER: A

42. WPA2 is used for security in
A. ethernet
B. bluetooth
C. wi-fi
D. none of the mentioned
ANSWER: C

43. An attempt to make a computer resource unavailable to its intended users is called
A. denial-of-service attack
B. virus attack
C. worms attack
D. botnet process
ANSWER: A

44. Pretty good privacy (PGP) is used in
A. browser security
B. email security
C. FTP security
D. none of the mentioned
ANSWER: B

45. PGP encrypts data by using a block cipher called
A. international data encryption algorithm
B. private data encryption algorithm
C. intrenet data encryption algorithm
D. none of the mentioned
ANSWER: A

46. Network layer firewall has two sub-categories as
A. State full firewall and stateless firewall
B. Bit oriented firewall and byte oriented firewall
C. Frame firewall and packet firewall
D. None of the mentioned
ANSWER: A

47. A firewall is installed at the point where the secure internal network and untrusted external network meet which is also known as _____
A. Chock point
B. Meeting point
C. Firewall point
D. Secure point
ANSWER: A

48. A proxy firewall filters at?
A. Physical layer
B. Data link layer
C. Network layer
D. Application layer
ANSWER: D

49. A packet filter firewall filters at?

A. Physical layer
B. Data link layer
C. Network layer or Transport layer
D. Application layer
ANSWER: C

50. The technology used to distribute service requests to resources is referred to as :
A. load performing
B. load scheduling
C. load balancing
D. All of the mentioned
ANSWER: C

51. Which of the following software can be used to implement load balancing ?
A. Apache mod_balancer
B. Apache mod_proxy_balancer
C. F6s Big IP
D. All of the mentioned
ANSWER: B

52. Wi-Fi stands for-
A. Wireless Fidelity
B. Wireless LAN
C. Wireless FLAN
D. None of the mentioned
ANSWER: A

53. When fraud access points are created to access information such as passwords. Which type of Wireless network threat would you classify this under?
A. Identity Theft
B. Network Injection
C. Man in the middle attack
D. Malicious Association
ANSWER: D

54. When bogus reconfiguration commands are used to affect routers and switches to degrade network performance. Which type of Wireless network threat would you classify this under?
A. Network Injection
B. Malicious Association
C. Man in the middle attack
D. Denial Of Service
ANSWER: A

55. When communication is unknowingly going through an adversary/intermediate. Which type of Wireless network threat would you classify this under?
A. Malicious Association
B. Man in the middle attack
C. Network Injection
D. Accidental Association
ANSWER: B

56. What special feature makes the smartcard so flexible to use?
A. the ability to protect stored information
B. the use of a microprocessor and programmable memory
C. the high speeds at which it is able to operate
D. the capability of storing huge amounts of information per unit of area
ANSWER: B

57. Which of the following does NOT use a 'Cryptographical Technique' to protect data?
A. the use of digital signatures
B. data encryption
C. the use of stored encrypted password files
D. using asymmetric keys at 'sender' and 'receiver' nodes
ANSWER: C

58. What characteristic makes the internet so attractive?
A. the 'secure' surroundings within which it is implemented
B. the ability to provide an open, easy-to-use network
C. it eliminates the need for firewalls
D. you don't require a fast computer to use the internet
ANSWER: B

59. Why is it important for the internet to implement protocols?
A. to provide a universal data 'platform' for all connections to use
B. so that nobody gets confused
C. to enable the use of cryptographical techniques
D. to prevent the use of viruses
ANSWER: A

60. Which of the following is NOT an example of a smartcard?
A. a credit card which can be used to operate a mobile phone
B. an electronic money card e.g Mondex
C. a drivers licence containing current information about bookings etc.
D. an access control card containing a digitised photo
ANSWER: D

61. Which of the following is the primary cause of 'invisible' damage? (i.e damage is of unknown extent)
A. viruses
B. computer misuse
C. computer fraud
D. theft
ANSWER: A

62. What type of signal is generally used, between the badge and sensor, in an active badge system?
A. radio waves
B. ultrasonic
C. satellite communication
D. infra-red
ANSWER: D

63. What method is used to receive information, from the sensor to the workstation, in an active badge system?

A. frequency division multiplexing
B. time division multiplexing
C. first-in first-out mechanism (FIFO)
D. random detection
ANSWER: C

64. Why will specific active badges NOT work with all active badge systems?
A. they operate at different frequencies
B. they use different coding mechanisms
C. they adopt different methods of transmission
D. they can only be used in certain environments
ANSWER: B

65. Which of the following methods can most effectively be used to prevent logical breach of security?
A. operating system and other system software
B. computer architectural design
C. distributed systems
D. network designdesign
ANSWER: A

66. Why are traditional authentication methods unsuitable for use in computer networks?
A. they do not use cryptographical techniques
B. they do not permit high speed data flow
C. they use passwords
D. they are incompatible with the internet
ANSWER: A

67. What can a firewall protect against?
A. viruses
B. unauthenticated interactive logins from the "outside" world
C. fire
D. connecting to and from the "outside" world
ANSWER: B

68. What is the main purpose of access control?
A. to authorise full access to authorised users
B. to limit the actions or operations that a legitimate user can perform
C. to stop unauthorised users accessing resources
D. d. to protect computers from viral infections
ANSWER: B

69. Which of the following is NOT a good property of a firewall?
A. only authorised traffic must be allowed to pass through it
B. the firewall itself, should be immune to penetration
C. it should allow for easy modification by authorised users
D. traffic must only be allowed to pass from inside to outside the firewall
ANSWER: D

70. All of the following are examples of real security and privacy risks EXCEPT
A. Viruses
B. Identity theft

C. Hackers
D. Spam
ANSWER: D

71. A person who uses his expertise to gain access to other people's computers to get information illegally or to cause damage is a
A. Programmer
B. Analyst
C. Spammer
D. Hacker
ANSWER: D

72. The common name for the crime of stealing passwords is
A. Jacking
B. Identify Theft
C. Spoofing
D. Hacking
ANSWER: C

73. What type of virus uses computer hosts to reproduce itself?
A. Time Bomb
B. Worm
C. Melissa virus
D. Macro Virus
ANSWER: B

74. Which of the following is an anti-virus program
A. Norton
B. K7
C. Quick heal
D. All of these
ANSWER: D

75. All of the following are examples of real security and privacy threats except:
A. Hackers
B. Virus
C. Spam
D. Worm
ANSWER: C

76. _____ monitors user activity on internet and transmit that information in the background to someone else.
A. Malware
B. Spyware
C. Adware
D. None of these
ANSWER: B

77. Viruses are _____.
A. Man made
B. Naturally occur

C. Machine made
D. All of the above
ANSWER: A

78. Which of the following is not an external threat to a computer or a computer network
A. Ignorance
B. Trojan horses
C. Adware
D. Crackers
ANSWER: A

79. When a person is harrassed repeatedly by being followed, called or be written to he / she is a target of
A. Bullying
B. Stalking
C. Identity theft
D. Phishing
ANSWER: B

80. Which of the following is a class of computer threat
A. Phishing
B. Soliciting
C. DoS attacks
D. Stalking
ANSWER: C

81. Which of the following is a Factors of authentication
A. Something You Know
B. Something You Have
C. Something You Are
D. all of the above
ANSWER: D

82. Each system shares one common attribute is _____
A. Public Key
B. Private Key
C. Index Key
D. All of the above
ANSWER: A

83. Simulating or Emulating a computer inside another computer using hardware and software.
A. Virtual machine
B. Virtual Server
C. Virtual Computer
D. None of the above
ANSWER: A

84. There are three primary types of RFID tags
A. One
B. Two
C. Three
D. Four

ANSWER: C

85. _____ tags activate when they receive a signal from the reader.
A. passive
B. battery-assisted passive
C. active
D. None of the above
ANSWER: A

86. Which RFID tags that operate without any battery power use the power in the signal sent by the reader to power them and send back their responses.
A. Passive Tags
B. Battery-Assisted Passive Tags
C. Active Tags
D. All of the above
ANSWER: A

87. Which RFID tags activate after the reader sends a signal, but use battery power to construct and send their responses.
A. Battery-assisted passive tags
B. Passive Tags
C. Active Tags
D. None
ANSWER: A

88. EPC tags are _____ RFID tags, and organizations frequently integrate them into stickers.
A. Battery-Assisted passive
B. Passive
C. Active
D. All of the above
ANSWER: B

89. EPC stands for
A. electronic product code
B. electronic project code.
C. electronic product compiler
D. election product code.
ANSWER: A

90. RFID-equipped with ID cards is
A. provax card
B. pro cards
C. proximity cards
D. All of the above
ANSWER: C

91. Why Attackers use proxies ?
A. Internet Protocol (IP) addresses are traceable
B. MAC addresses are traceable
C. VPN addresses are traceable
D. all of the above

ANSWER: A

92. IPSec is designed to provide the security at the
A. transport layer
B. network layer
C. application layer
D. session layer
ANSWER: B

93. In tunnel mode IPsec protects the
A. Entire IP packet
B. IP header
C. IP payload
D. None of the mentioned
ANSWER: A

94. Network layer firewall works as a
A. frame filter
B. packet filter
C. both (a) and (b)
D. none of the mentioned
ANSWER: B

95. Network layer firewall has two sub-categories as
A. stateful firewall and stateless firewall
B. bit oriented firewall and byte oriented firewall
C. frame firewall and packet firewall
D. none of the mentioned
ANSWER: A

96. What is BotNet?
A. A botnet nothing but internet.
B. A bot is a single node added to a network of other infected systems
C. Both (a) and (b)
D. None
ANSWER: B

97. WPA2 is used for security in
A. ethernet
B. bluetooth
C. wi-fi
D. none of the mentioned
ANSWER: C

98. ------- are often delivered to a PC through an email attachment and are often designed to do harm.
A. Spam
B. Email
C. Portals
D. Virus
ANSWER: D

99. The altering of data so that it is not usable unless the changes are undone is
A. ergonomics
B. compression
C. biometrics
D. encryption
ANSWER: D

100. When a logic bomb is activated by a time related event, it is known as -------
A. virus
B. trojan horse
C. time related bomb sequence
D. time bomb
ANSWER: D

101. An attempt to make a computer resource unavailable to its intended users is called
A. denial-of-service attack
B. virus attack
C. worms attack
D. botnet process
ANSWER: A

102. Authentication is
A. modification
B. insertion
C. hard to assure identity of user on a remote system
D. none of the above
ANSWER: C

103. -------- are attempts by individuals to obtain confidential information from you to falsifying their identity.
A. Computer viruses
B. Phishing scams
C. Phishing trips
D. Spyware scams
ANSWER: B

104. A virus that migrates freely within a large population of unauthorized email user is called a -------
A. flame war
B. worm
C. macro
D. plagiarism
ANSWER: C

105. What is short for malicious software (is software designed to disrupt computer operation, gather sensitive information, or gain unauthorized access to computer systems)?
A. Malware
B. Moleculewar
C. Malisoft
D. Malairasoft
ANSWER: A

106. Extensible authentication protocol is authentication framework frequently used in
A. wired personal area network
B. wireless networks
C. wired local area network
D. none of the mentioned
ANSWER: B

107. Which of the following virus overtake computer system, when it boots and destroy information?
A. System infectors
B. Trojan
C. Boot infectors
D. Stealth virus
ANSWER: D

108. Key logger is a
A. Firmware
B. Antivirus
C. Spyware
D. All of the above
ANSWER: C

109. To protect yourself from computer hacker, you should turn on a
A. Script
B. Firewall
C. VLC
D. Antivirus
ANSWER: B

110. Firewalls are used to protect against --------
A. data driven attacks
B. fire attacks
C. virus attacks
D. unauthorised access
ANSWER: D

111. Pretty good privacy (PGP) is used in
A. browser security
B. email security
C. FTP security
D. none of the mentioned
ANSWER: B

112. PGP encrypts data by using a block cipher called
A. international data encryption algorithm
B. private data encryption algorithm
C. intrenet data encryption algorithm
D. none of the mentioned
ANSWER: A

113. When a DNS server accepts and uses incorrect information from a host that has no authority giving that information, then it is called

A. DNS lookup
B. DNS hijacking
C. DNS spoofing
D. None of the mentioned
ANSWER: C

114. In cryptography, what is cipher?
A. algorithm for performing encryption and decryption
B. encrypted message
C. both (a) and (b)
D. none of the mentioned
ANSWER: A

115. In computer security----------means that computer system assets can be modified only by authorized parities.
A. Confidentiality
B. Integrity
C. Availability
D. Authenticity
ANSWER: B

116. In computer security---------- means that the information in a computer system only be accessible for reading by authorized parities.
A. Confidentiality
B. Integrity
C. Availability
D. Authenticity
ANSWER: A

117. The type of threats on the security of a computer system or network are ---------- i) Interruption ii) Interception iii) Modification iv) Creation v) Fabrication
A. i, ii, iii and iv only
B. ii, iii, iv and v only
C. i, ii, iii and v only
D. All i, ii, iii, iv and v
ANSWER: C

118. Which of the following is independent malicious program that need not any host program?
A. Trap doors
B. Trojan horse
C. Virus
D. Worm
ANSWER: D

119. The ------ is code that recognizes some special sequence of input or is triggered by being run from a certain user ID of by unlikely sequence of events.
A. Trap doors
B. Trojan horse
C. Logic Bomb
D. Virus
ANSWER: A

120. The ---------- is code embedded in some legitimate program that is set to explode when certain conditions are met.
A. Trap doors
B. Trojan horse
C. Logic Bomb
D. Virus
ANSWER: C

121. Which of the following malicious program do not replicate automatically?
A. Trojan Horse
B. Virus
C. Worm
D. Zombie
ANSWER: A

122. In asymmetric key cryptography, the private key is kept by
A. sender
B. receiver
C. sender and receiver
D. all the connected devices to the network
ANSWER: B

123. Which one of the following algorithm is not used in asymmetric-key cryptography?
A. rsa algorithm
B. diffie-hellman algorithm
C. electronic code book algorithm
D. none of the mentioned
ANSWER: C

124. What is data encryption standard (DES)?
A. stream cipher
B. block cipher
C. bit cipher
D. none of the mentioned
ANSWER: B

125. State whether true of false. i) A worm mails a copy of itself to other systems. ii) A worm executes a copy of itself on another system.
A. True, False
B. False, True
C. True, True
D. False, False
ANSWER: C

126. The common name for the crime of stealing passwords is
A. Jacking
B. Identify Theft
C. Spoofing
D. Hacking
ANSWER: C

127. What is the name of an application program that gathers user information and sends it to someone through the Internet?
A. Virus
B. Spybot
C. Logic Bomb
D. Security Patch
ANSWER: B

128. Which one of the following is a cryptographic protocol used to secure HTTP connection?
A. stream control transmission protocol (SCTP)
B. transport layer security (TSL)
C. explicit congestion notification (ECN)
D. resource reservation protocol
ANSWER: B

129. ElGamal encryption system is
A. symmetric key encryption algorithm
B. asymmetric key encryption algorithm
C. not an encryption algorithm
D. none of the mentioned
ANSWER: B

130. Confidentiality with asymmetric-key cryptosystem has its own
A. System
B. Data
C. Problems
D. Issues
ANSWER: C

131. SHA-l has a message digest of
A. 160 bits
B. 512 bits
C. 628 bits
D. 820 bits
ANSWER: A

132. Message authentication is a service beyond
A. Message Confidentiality
B. Message Integrity
C. Message Splashing
D. Message Sending
ANSWER: B

133. In Message Confidentiality, transmitted message must make sense to only intended
A. Receiver
B. Sender
C. Third Party
D. Translator
ANSWER: A

134. A hash function guarantees integrity of a message. It guarantees that message has not be
A. Replaced
B. Over view
C. Changed
D. Left
ANSWER: C

135. To check integrity of a message, or document, receiver creates the
A. Tag
B. Hash Tag
C. Hyper Text
D. Finger Print
ANSWER: B

136. A digital signature needs a
A. private-key system
B. shared-key system
C. public-key system
D. All of them
ANSWER: C

137. One way to preserve integrity of a document is through use of a
A. Thumb Impression
B. Finger Print
C. Biometric
D. X-Rays
ANSWER: B

138. A session symmetric key between two parties is used
A. only once
B. twice
C. multiple times
D. depends on situation
ANSWER: A

139. Encryption and decryption provide secrecy, or confidentiality, but not
A. Authentication
B. Integrity
C. Keys
D. Frames
ANSWER: B

140. MAC stands for
A. message authentication code
B. message authentication connection
C. message authentication control
D. message authentication cipher
ANSWER: A

141. Digest created by a hash function is normally called a
A. modification detection code (MDC)

B. message authentication connection
C. message authentication control
D. message authentication cipher
ANSWER: A

142. Message confidentiality is using
A. Cipher Text
B. Cipher
C. Symmetric-Key
D. Asymmetric-Key
ANSWER: D

143. A sender must not be able to deny sending a message that he or she, in fact, did send, is known as
A. Message Nonrepudiation
B. Message Integrity
C. Message Confidentiality
D. Message Sending
ANSWER: A

144. To preserve integrity of a document, both document and fingerprint are
A. Important
B. System
C. Needed
D. Not needed\
ANSWER: C

145. In Message Integrity, SHA-l hash algorithms create an N-bit message digest out of a message of
A. 512 Bit Blocks
B. 1001 Bit Blocks
C. 1510 Bit Blocks
D. 2020 Bit Blocks
ANSWER: A

146. . Cryptographic hash function takes an arbitrary block of data and returns
A. fixed size bit string
B. variable size bit string
C. both (a) and (b)
D. none of the mentioned
ANSWER: A

147. Message confidentiality or privacy means that sender and receiver expect
A. Integrity
B. Confidentiality
C. Authentication
D. Nonrepudiation
ANSWER: B

148. protocols are?
A. Agreements on how communication components and DTE's are to communicate 77%
B. Logical communication channels for transferring data 11%
C. Physical communication channels sued for transferring data 9%

D. None of above
ANSWER: A

149. Which of the following pieces of information can be found in the IP header?
A. Source address of the IP packet
B. Destination address for the IP packet
C. Sequence number of the IP packet
D. Both (A) and (B) only.
ANSWER: D

150. I bank online. Which of the following are application-level encryption protocols that I would most likely use to securely bank online?
A. SSL and SET
B. Verisign and SHA1
C. READY, SET, and GO
D. PGP, PEM, and SSL
ANSWER: A

Staff Name
Premkumar.A.