4th Year 1st Sem 2nd Mid Online Bits
For CSE
CN

1. A connection is a transport that provides :> **A Suitable type of service between client and server**
2. A Form of virus that hide itself from antivirus program:>**Stealth virus**
3. A Form of virus that mutates with every infection is :> **Polymorphic virus**
4. A full service Kerberos environment is callcd.->**Realm**
5. A person who is a legitimate user but also tries to acess some unauthorized aocess:>**Misfeasor**
6. A person who is not authorized to use the system but penctrates:->**Masqnarader**
7. A person who takes supervisory control of the system is:->**Clandestinc user**
8. A secret entry point in to an application is:->**Trapdoor**
9. A session is a transport that provide:> **An association between service between client**
10. A software basal logical or virtual computer is:->**CPU Emulator**
11. Absolute requirement of Specification is called:>**MUST**
12. AH Represcnts:->**Authenticated Header**
13. Alert protocol uses :>**2 bytes**
14. An entity that ss capable of An entity that is capable of accessing objects is:->**subject**
15. An expert system is involved :>**peneteratio Identification system**
16. Anti replay mechanism uses the window size of:->**w**
17. Application gateway is also Application gateway is also called as:->**Proxy server**
18. Application more than security protocol to the same IP packet without invoking tunneling is known as :>**Transport adjacency**
19. Application of multiple layer of security protocols effected through IP tummeling is known as:> **Iterated Tunneling**
20. Application of one way Authentication js;-**>Email**
21. AS Represents:->**Authenticalion server**
22. Authentication of encryption is apply to IP header is not protected in:> **Transport mode** ESP
23. Book 1 of the SET specification gives:>**Business Description**
24. Book 2 of the SET specification gives :> **Programmers guide**
25. Book 3 of the SET specification gives :> **Formal protocol definition**
26. Certificate verify messageuses the parameter:>**Signature**
27. Certificates generated by A that are the certificates of other certificate Authorities is:->**Reverse Certificates**
28. Certificates of A generated by other certificate Authorities is called:->**Forward Certificates**
29. Change eipher specified protocol uses :>**1 byte**
30. Changing the contents of message is called :>**Modification**
31. Combination of SHA-1 and RSA provides an effective:->**DigitaI Signature**
32. Cryptanalysis of hash functions focus on:->Internal structure of compression function f
33. Denying of message by destination is ca]]cd:->**Repudiation**
34. DES uses the key size as :>**56 bits**
35. Digital immune system was developed by:->**IBM**
36. DOI Represents:->**Domain of Interpretation**
37. DSA Represents:>**Digilal signature algorithm**
38. Each round in MD5 has:>**16 steps**
39. Each round in SHA-1 is having **:->20 steps**
40. ESP represent:> **Encapsulation security payload**
41. Execution denial measure comes under:->**File access activity**
42. Explodes when certain conditions me:>**Logic bomb**
43. First generation antivirus approach uses:>**Simple scanners**
44. For encrypting session keys the algorithm used by MLA in S/MIME represents:->**Diffie Hellman**
45. For message encryption and decryption algorithm in S/MIME is:->**Triple DES**
46. Fortezza uses the key she a:>**80 bits**
47. Frequency of occurrences of various events observed m:>**TIircshold detection model**
48. Handshke protocol uses:>**10**
49. Hash function can be applied to a block of:->**Variable size**
50. **H**MAC is used in:->**Transport layer security**
51. In Direct Digital Signature the destination knows:>**Source Public Key**
52. In PGP DC Refers to:->**Private Key Decryption**

53. In PGP DP Refers to:->**Public Key Decryption**
54. In PGP EC Refers to:->**Private Key Encryption**
55. In PGP EP Refers to:->**Public Key Encryption**
56. In S/MIME for encrypting Digital Signature MUST support …….algorithm:>**MD5**
57. In S/MIME for encrypting Digital signature SHOULD support ……..algorithm:>**MD5**
58. In source station specifies the route that packet should follow over:>**source routing attacks**
59. In the construction of dual signature it uses the encryption algorithm:> **RSA**
60. In the construction of dual signature it uses the hash algorithm:>**SHA-1**
61. In time stamp mechanism the source uses:>**garbage value**
62. Inserting of data in to the network from Unauthorised persons is called.'>**Masquerade**
63. Integrity check value is a authentication code produced by:> **MAC**
64. IP Security encompasses:->**Authcntication**
65. IP Security is provided in:->**Network layer**
66. Ipad value in HMAC is:->**00110110**
67. It is the one It is the one to which access is controlled:->**object**
68. It is the way m which an object is access by a subject:->**Access rights**
69. IV Represents the:->**Initial Vector**
70. Kerberos is:-> **Authentication service**
71. Kerberos makes use of the algorithm:->**DES**
72. Kerberos provide s the following:->**Centralized Authenticated server**
73. Kerberos version **4** depends on the prolocol>>**IP**
74. Key legimacy field of public key ring sJSTtfij is used for:->**Trust**
75. Life time in a ticket refers:->**I.ength of the time for which ticket is valid**
76. MAC is also called as>>**Mcssagc digest**
77. MAC Represents:> **Message Authentication code**
78. MD**5** algorithm maps a message a block of **512** bits:>**128 bits message digest**
79. MD**5** Algorithum is developed by>>**Ron Rivest**
80. Message byte ordering of Kcrbcros version 4:>**Ambiguous byte ordering**
81. MIME version parameter value is:->**1.0**
82. MLA in S/MIME represents:> **Mail List Agent**
83. Multi variate model is based on:->**eorclations**
84. Nonce is a :> **Locally generated pseucode random number**
85. Number of rounds in RIPEMD-160 algorithm are:->**10**
86. Number of rounds in SHA-l algorithm are**:->4**
87. OAKLEY is a refinement of the :>**Diffie Hellman**
88. One among the following is not a firewall:->**network gate**
89. One of the new fields added to version 2 of X.509 is:->**Subject unique identifier**
90. One of the new fields added to version 3 ofX.509 is:->**Extension**
91. Opad value in HMAC is:->**01011100**
92. Packet filtering router applies rules on incoming:->**IP packet**
93. Password of UNIX system typically contains:>**56 bits**
94. Period of validity in X.509 format contains:->**Two number of dates**
95. Platform independent virus is :> **macro virus**
96. PRC means:->**Privatc cycle block chaining** .
97. Process of mapping variable to fixed size called as :>**Flashing Function**
98. Profile based detection comes under>>**C Stalistical anomaly detection system**
99. Providing support to remotenhostnis done in:>**case 4**
100. Pseudo code is explained by:->**Boer**
101. Purpose client/Server Authentication,cxchangc:->**Used to obtain service**
102. Purpose of Authentication service exchange is:->**Used to obtain ticket granting ticket**
103. Purpose of ticket Granting service exchange is:->**Used to obtain service granting ticket**
104. Quantity of output to location is a measure in:->**Login and session activity**
105. RC4-40 uses the key size as:>**40 bits**
106. Releasing of message to Unauthorized persons is called;->**Disclosure**
107. Rules are developed to detect deviation from previous usage model ui:->**Anomaly Detection**
108. S/MIME does not provide the following functionality:> **Local data**
109. Salt value of UNIX system typically contains:->**12 bits**
110. Second generation antivirus approach uses:>**Heuristic scanners**
111. Security is provided between gateways is :>**case2**
112. SET is an open encryption designed to protect on the internet :>**Credit card transcation**
113. SHA Represents:->**Secure hash Algorithm**
114. S**H**A Uses buffer register of sizc:->**160 bits**
115. Size of Single buffer register in MD**5** ts:->**32bits**

116. Size of the sequence number counter is:->**32 bits**
117. Socks server runs on the firewall.->**UNIX based**
118. SOCKS service is Iocated:->**TCP port 108**
119. SPI Represents:->**Security parameter Index**
120. SSL is the security provided at :>**Network layer**
121. SSl was orginated by :> **Netscape**
122. Structure of private key ring contains:->**5 fields**
123. Structure of public key ring contains:->**8 fields**
124. TGS stands for:->**Tickct Grating server**
125. The algorithm that is used for email compatibility in PGP is:->**Radix-464 conversion**
126. The basic combination of the security provided between end system is:>**casel**
127. The basic element of data acess control is:>**Subject**
128. The buffer registers used by SHA**-1** for holding intermediate and final results:>**5**
129. The column in the access matrix represents:->**object**
130. The column wise decomposition of access matrix gives:->**Access Control list**
131. The default actions taken by packet filter ing are:>**Discard and forward**
132. The Digital signature slgorithm uses:> **Users private key**
133. The entries in the access matrix represents:->**access right**
134. The first kind of defence against intruders is:->**password system**
135. The function which is used for message storage or transmission:>**Comprcssion**
136. The lime stamp in a ticket contains:->**both Date and time**
137. The major version of SSL is :> **Three**
138. The major version of TLS is:> **Three**
139. The max allowable MAC length in SSl Record protocol is**:>210 bytes**
140. The max fragment block size in SSl is:>**214 bytes**
141. **The** Maximum allowable padding length in MD**5**:->**up to 512** bit
142. The minor version of SSl is :> **Zero**
143. The minor version of TLS is:> **ONE**
144. The Model that is used to establish transition probabilities among various states:->**Markov model**
145. The number of additive constans Is used by MD**5** are**:->64 173.**
146. The number of additive constants used by RIPEMD are**:->9**
147. The number of additive constants used by SHA**-1** are;->**4.**
148. **The** number of buffer registers used by M**D5** are**:>4**
149. The number of key exchanges in ISAKMP are:>**5**
150. The number of primitive logical functions used by MD**4** arc**:->4**
151. The number of public key algorithms in S/MI:>**3**
152. The number of rounds in MD**4 are:>4**
153. The number of rounds in MD**5** are**;->4**
154. The number of tickets in More authentication dialogue of Kerberous version 4 are :>**two**
155. **The** number of tickets **in** simple authentication dialogue of Kerberous version 4 are:> **one**
156. The number of versions in Kerberos are:->**Five**
157. The number of versions in X.509 are:->**Three**
158. The payload length field is ISAKMP is :>**2 bytes**
159. The primitive function used in round 3 of MD5 are:->**B XOR C XOR D**
160. The requirement that the user should aware that authentication is taking place is called as:>>**Transparent**
161. The routing protocol used by IP security is :>**OSPF**
162. The row wise decomposition of access matrix gives:->**Capabilitv Tickets**
163. The rows in the access matrix represents:->**subject**
164. The SHA-1 algorithm allows the maximum input message length less than:->**263**
165. The SHA-1algorithm outputs the message digest of:>**160**
166. Third generation antivirus approach uses:->**Activity traps**
167. Third generation antivirus approach uses:->**Full featured**
168. This error isa not present in the fatal error of TLS:>**Close notify**
169. Threshold detection comes under:->C Statistical anomaly detection system :> **51.**
170. Tiie maximum life time of ticket in Kerberos version **5** is:->**Arbitary life limes**
171. Time stamp is used to protect against:->**Replay attack**
172. TLS is the security provided at:>**Transport layer**
173. To ensure against attacks Oakrlay employs :> **None**
174. Total Number of Steps in MD5 arc:->**64**
175. Total Number of Steps in R**I**PEMD-I**6**0 are**:>16**
176. Total Number of Steps in SHA**-1** urc**:->80**
177. Tunnel mode provides protection to:->**Entire IP Packet**
178. Version 5 of Kerberos uses the encryption mode:->**CBC**
179. Version 5 of SOCKS is defined in:>**RFC 1928**

180. Virus places identical copy of itself into another program is:>**propogation phase**
181. Which among the follow controls the execution of target code :>**Emulation control**
182. Which among the following key exchange in ISAKMP contains a single message:>**Authentication exchange**
183. Which of the following algorithm is faster>>**MD5**
184. Which of the following checks for known viruses:-> **Virus signature scanner**
185. Which of the following does not need host program:->**Worm**
186. Which of the following exchange scenario is not for message exchange of Kerberos version 4: >**Server service exchange**
187. Which of the following formal is used by SHA-1 for storing values in buffer registers:>**Big Endian**
188. Which **of** the following format is used by MD**5** for storing values In buffer registers:>**Little Endian**
189. Which of the following format is used by RIPEMD-**160** for storing values in buffer registers:> **Little Indian**
190. Which of the following gives an over view of security Architecture **:> RFC 1825**
191. Which of the following gives an over view of security encryption mechanismsecurity Architecture:>**RFC 1829**
192. Which of the following is not a field of private key ring structure:->**Owner test**
193. Which of the following is not a field of pub cey ring structure:->**Encryptcd private key**
194. Which of the following is not a good metric that is useful for profile based intrusion detection- >**Library**
195. Which of the following is not a phase of Virus:>**Dedicated Phase**
196. Which of the following is not a valid authentication procedure:->**Zero way Authentication**
197. Which of the following operation is used by Simple hash function to generate hash code.- >**XOR**
198. Which of the followings is not requirement of Kerberos:->**Discovery**
199. Which will depend on past audit records:->**Operational model**
200. X.509 is is>**Public Key certificate**