# 4th B TECH 1ST SEM 1ST MID (R10)
## CNS

1. In general the number of keys used by private key encryption algorithm :->**1**
2. In general the number of keys used by private key encryption algorithm :->**1**
3. Which of the following allows key exchange with out real time access to Public key Authority :->**Public key certificates**
4. RSA extended the work of :->**Diffie and Hellman**
5. This will accept the cipher text and the matching key and produces the plain text :->**Decryption**
6. The scrambled message that is produced as output :->**Cipher tex**
7. The readable message or data that is fed in to the algorithm as input :->**Plain tex**
8. Which of the Public key crypto system uses Key exchange :-> **Diffie Hellman**
9. Which of the Public key crypto system do not uses Key exchange :->**DSS**
10. RSA algorithm is not based on :->**Ring numbers**
11. Simplest secret key distribution is proposed by :->**Merkle**
12. In Public key certificates signatures can be verified by any one who knows the public key or :->**Certificate Authority**
13. The number of public global elements in Diffie Hellman key exchange algorithm :->**2**
14. The key used in conventional encryption is referred as :->**Secret key**
15. Public key encryption is also called as :->**Asymmetric encryption**
16. In which of the following one of the two keys must kept secret :->**Public key encryption**
17. Which of the Public key crypto system uses Digital Signature :->**Elliptic curve**
18. ECC stands for :-> **elliptic curve cryptography**
19. ECC stands for :-> **elliptic curve cryptography**
20. ECC rely on the difficulty of solving elliptic curve :->**Discrete logarithm problem**
21. Elliptic curve cryptography was introduced by :-> **Miller**
22. Which of the following algorithm technique is based on elliptic curve:->**Elliptic curve algorithm**
23. Which of the Public key crypto system uses Key exchange :->**Elliptic curve**
24. In which of the following The sender and receiver uses matched pair of keys :->**Public key encryption**
25. In which of the following The sender and receiver uses the different algorithm:->**Public key encryption**
26. Which of the Public key crypto system uses Digital Signature :->**RSA**
27. Which of the Public key crypto system uses Digital Signature :->**DSS**
28. Which of the Public key crypto system do not uses Digital Signature :-> **Diffie Hellman**
29. Which of the following algorithm is not used for either encryption or key exchange:->**DSS**
30. NIST stands for :-> **National institute of Standards**
31. Which algorithm enables two users to exchange a secret key securely that can be used for subsequent encryption of messages :->**Diffie Hellman**
32. Which of the following algorithm is not used for either encryption or key exchange:->**DSS**
33. NIST stands for :-> **National institute of Standards**
34. In RSA algorithm Euler Totient è(n)= :-> **(p-1)*(q-1)**
35. Conventional encryption is also called as :->**symmetric encryption**
36. In which of the following The shared key must kept secret :->**Conventional encryption**
37. Which of the Public key crypto system uses Encryption or decryption :->**RSA**
38. Which of the Public key crypto system uses Encryption or decryption :->**Elliptic curve**
39. if p=17 and q= 11 then Private key in RSA algorithm is :->**{23,187}**
40. if p=17 and q= 11 then Public key in RSA algorithm is :->**{7,187}**
41. if p=17 and q= 11 then ∅(n) in RSA algorithm is:->**160**
42. In RSA algorithm Private key KR= :-> **{d,n}**

43. In RSA algorithm public key KU= :-> **{e,n}**
44. RSA is a block cipher in which the plain text and cipher text are integers between :->**0 and n-1**
45. Which of the Public key crypto system uses Key exchange :-> **RSA**
46. In which of the following The sender and receiver uses the same key :->**Conventional encryption**
47. Which of the Public key crypto system uses Key exchange :-> **RSA**
48. Which of the Public key crypto system do not uses Encryption or decryption :->**DSS**
49. Which of the Public key crypto system do not uses Encryption or decryption :-> **Diffie hellman**
50. For n =8 then ∅(8)= :->**4**
51. For n =6 then ∅(6)= :->**2**
52. (11 mod 8 * 15 mod 8 ) mod 8= :->**5**
53. [(a mod n) * (b mod n)] mod n= :->**(a*b) mod n**
54. ∅(n) in Euler Totient function represents :->**number of integers lesser than n relative prime to n**
55. For n =7 then ∅(7)=:->**6**
56. gcd(60,24)= :->**12**
57. gcd (a,0)= :->**|a|**
58. if two numbers share no factors in common other than 1 then they are said to be :->Relative **Prime**
59. if (a*b)=(a*c) mod n then b= c mod n, if a is :->**Congruent modulo**
60. For n =9 then è(9)= :->**6**
61. For n= 1 then ∅(1)= :->**1**
62. For n =9 then∅(9)= :->**6**
63. For two prime numbers p and q for n=pq then è(n)is not equal to :->**p*q**
64. if p is prime then ∅(p)= :-> **p-1**
65. For n =10 then ∅(10)= :->**4**
66. [(a mod n) - (b mod n)] mod n= :->**(a-b ) mod n**
67. [(a mod n) + (b mod n)] mod n= :->**(a+b) mod n**
68. 11 mod 8= :->**3**
69. (0+a) mod n=a mod n is :->**Additive identity**
70. a mod n= b mod n implies :->**a=b mod n**
71. Two integers a and b are said to be congruent modulo if :->**a mod n= b mod n**
72. (a+b) mod n= (b+a) mod n is :->**Commutative**
73. GCD (a,b)= :->**(|a|,|b|)**
74. Given a and b are integers , if a= mb then b is :->**Divisor of a**
75. Number Theory is mainly concentrate on :->**Prime Numbers**
76. Two numbers a and b are said to be relatively prime if gcd(a,b)= :->**1**
77. An integer p is having only divisors +1,-1,+p and p , then p is called as :->**Prime number**
78. Which of the following numbers are relative prime :->**15,28**
79. Number theory is essential to which of the following cryptographic algorithms:->**Public key**
80. Common things of DES, Blow fish and CAST-128 algorithm is :->**Blow fish**
81. Rotation Operation is not found in the following algorithm :->**Blow fish**
82. Addition Operation is not found in the following algorithm :->**Triple DES**
83. Maximum number of bits for key size in Blow fish algorithm are:->**32**
84. Brue Schnier developed the following algorithm :->**Blow fish**
85. Key dependent S-Boxes are used in the following algorithm :->**BlowFish**
86. Key dependent operations are found in the following algorithm :->**CAST-128**
87. Variable S-boxes are allowed for the following algorithm :->**Blow fish**
88. The best possible Avalanche effect is given to Blow fish by :->**Fuction F**

Which of the following algorithm not uses fixed S-boxes :->Blow fish
90. Maximum number of rounds in RC5 are :->255
91. Maximum Number of rounds is possible for the following algorithm :->Blow fish
92. Maximum key size is provided for the following algorithm :->RC5
93. Variable key is not provided for the following algorithm :-> IDEA
94. Variable block size is a property of the following algorithm:->RC5
95. Common things for DES, Triple DES and Blow Fish algorithm is :-> Same Block size
96. The key size of IDEA Algorithm is :->128
97. The total number of sub keys used in IDEA algorithm is :->52
98. An IDEA diffusion is provided by:->Multiplication structure
99. The number of sub keys that the output transformation of IDEA algorithm uses :->4
100. Which of the following cipher block mode is easy to analyse :->OFB
101. Which among the following is not a condition for block cipher :->Delay
102. Which of the following cipher block mode there is no protection on order of blocks :->ECB
103. Which of the following cipher block mode pad mechanism is not dependant on input bits :->OFB
104. Which of the following cipher block mode is not length preserving :->CCB
105. Which of the following cipher block mode is Finite Automaton with internal feed back :->OFB
106. Which of the following cipher block mode pad mechanism is dependant on input bits :->CFB
107. Which of the following cipher block mode suffers from Serial encryption :->CCB
108. Which of the following cipher block mode is not used to provide integrity :->CBC
109. Which of the following cipher block mode is used to provide integrity :->OCM
110. One of the following is not a valid operation in the scheme of simple DES :->Inverse initial substitution
111. NBS Stands for :->National Bureau of standard
112. The order of search for Differential Cryptanalysis is same as :->Differential Cryptanalysis
113. Differential Cryptanalysis is a :->Chosen Plain text
114. Exhaustive key search is a :-> Key attack
115. Linear Cryptanalysis is a :->Known plain text
116. Which one among the following is not a n approach that is used to Strengthen the DES is :->Quadruple DES
117. Which one among the following is not a factor that is used to analyze the Strength of DES is :->Binary Cryptanalysis
118. The order of search for Linear Cryptanalysis is same as :->Differential Cryptanalysis
119. Linear Cryptanalysis was discovered by :->Matsui
120. one of the best application that uses DES is :->ATM
121. The number of bits for a plain text in DES contains :->64 bits
122. The number of bits for a plaintext in Simple -DES contains :->8 bits
123. DES is a :->Private key Algorithm
124. DES Stands for :->Data Encryption standard
125. Number of keys used in DES algorithm is :->1 key
126. Key length of DES Algorithm is :->56 bits
127. Each S-box takes 6 bits input and produces as output :->4
128. Number of S-Boxes used in DES algorithm is :->8
129. Number of sub keys generated in DES algorithm is :->16 keys
130. Which one among the following is not a Symmetric block cipher :->RC4
131. Which among the following is not a block cipher:->RC4
132. Substitution permutation was first introduced by :->Shanon
133. Which among the following ciphers operates on a single chunk of plain text :->Block cipher
134. The terms Confusion and Diffusion are introduced by :->Claude Shanner
135. One of the following is not a Condition that is used for evaluation of block cipher:-> Latency
136. Which of the following cipher Processes the input elements continuously producing output on

element at a time :->**Stream cipher**

137. A type of symmetric key encryption algorithm in which a block of bits is encrypted at a time and a cipher text of the same block is formed. :->**Block cipher**
138. Which among the following is needed in order to make the relationship between the statistics of Cipher text and the value of encryption key as complex as possible :->**Confusion**
139. In which of the following the statistical structure of the plain text is dissipated in to long range statistics of the cipher text:->**Diffusion**
140. Which among the following is not a Symmetric key encryption method :->**Public key**
141. Transposition cipher is a :->**Symmetric key encryption**
142. A technique in which the permutation is applied on letters of plaintext column wise is :-> **Column Transposition**
143. A technique in which the permutation is applied on letters of plaintext row wise is :->**Row Transposition**
144. which is simplest of such cipher, in which the plaintext is written down as a sequence of diagonals and then read off as a sequence of rows :->**Rail Fence**
145. Which one of the following is a permutation Cipher :->**Transposition**
146. Which among the following is not a transposition cipher :->**Play fair Cipher**
147. A technique in which the permutation is applied on letters of plaintext is :->**Transposition**
148. The cipher text for the plain text meet at the school house using Row Transposition Ciphers :->**ESOTCUEEHMHILAHSTOETO**
149. The cipher text for the plain text meet at the school house using Rail fence cipher is:->**MEATECOLOSETTHSHOHUE**
150. Which among the following is not a substitution cipher :->**Rail Fence**
151. Which of the following cipher requires a very long key which is expensive to produce and expensive to transmit. :->**One Time Pad Cipher**
152. Caesar cipher is also known as :->**shift Cipher**
153. The following Cipher involves replacing each letter of the alphabet with the letter standing three places further down the alphabet. :->**Caesar**
154. A technique in which the letters of plaintext are replaced by other letters or by numbers or symbols is :->**Substitution**
155. Which of the following cipher is based on linear algebra :->**Hill**
156. In which of the following cipher there are multiple cipher text letters for each plaintext letter :->**Vigenere cipher**
157. Which among the following is not a Substitution cipher :->**Rail fence**
158. The Caesar cipher for the plain text work :->**XRUN**
159. In which of the following cipher Frequency analysis is much more difficult :->**Play fair**
160. If an attacker attempts to alter the route tables remotely then it is :->**Route table modification attack**
161. Which type of attacks are often concerned with SSHL and SSL connection types :->**Man in the middle attack**
162. Which one among the following refers to the attacks performed on the ongoing packets across the machine.:->**ARP attack**
163. This is a Situation that ours when the amount of data that is placed in the memory is greater Than the amount of storage space actually allocated :->**Buffer overflow**
164. The field of both cryptography and cryptanalysis is :->**cryptology**
165. Which one among the following refers to the ability of an attacker for capturing certain portions of an ongoing session with in the network and to behave as one of the participants :->**Session Hijacking**
166. Which among the following same key is used for both Encryption and Decryption :->**Symmetric key**
167. Prevents or inhibits the normal use or management of communication facilities is :->**Denial of**

**service**

168. The cryptanalyst has a copy of the cipher text and the corresponding plaintext is :->**Known plaintext**
169. It processes the input elements continuously, producing output element one at a time, as it goes along. :->**stream cipher**
170. Converting plaintext to cipher text is :->**Encryption**
171. These attacks involve some modification of the data stream or the creation of a false stream:->**Active attack**
172. A mechanism that is designed to detect, prevent or recover from a security attack.:->**Security mechanism**
173. Any action that compromises the security of information owned by an organization is known as :->**Security attack**
174. Model of Network Security does not require one among the following :->**transmitting the secre information through in secure channel**
175. Which One among the following is not a Security Service :-> **Digital Signature**
176. Which One among the following is not a Security Mechanism :->**Authentication**
177. Which One among the following is an attack on Integrity :-> **Modification**
178. Which One among the following is not a Security Service :->**Digital Signature**