Subject:-INS (information Network security) TYCS SEM:-5

Sample Question

1) In _____ 2 different keys are implemented for encrypting as well as decrypting that particular information.

a) Symmetric Key Encryption

b) Asymmetric Key Encryption

c) Asymmetric Key Decryption

d) Hash-based Key Encryption

2)_____ is the mathematical procedure or algorithm which produces a cipher-text for any specified plaintext.

a) Encryption Algorithm

b) Decryption Algorithm

c) Hashing Algorithm

d) Tuning Algorithm

3) The _____ has piece of the keyword that has the same length as that of the plaintext.

a) Block Cipher

b) One-time pad

c) Hash functions

d) Vigenere Cipher

4) 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

5) Number of Round in DES algorithms?

a) 16

b) 20

c) 10

d) 12

6) What is sniffing?

a. Sending corrupted data on the network to trick a system

b. Capturing and deciphering traffic on a network

c. Corrupting the ARP cache on a target system

d. Performing a password-cracking attack

7)_____ is the art & science of cracking the cipher-text without knowing the key.

a) Cracking

b) Cryptanalysis

c) Cryptography

d) Crypto-hacking

8)Which key used by AES algorithm for encryption and decryption?

a) Symmetric key

b) Asymmetric key

c) Both a and b.

d) Un-know key

9) Which of the following is/are methods of providing secure communication between two entities through the use of mathematical coding?

a) Digital signature encryption

b) Public key encryption

c) Private Key encryption

d) All of the above

10)Diffie-Hellman algorithm is used for

a) Digital signature

b) Encryption

c) Decryption

d) Key exchange

11) Authority who is trusted to provide public key Certificate to Merchant, Card holder and Payment gateway?

a) Serial Authority.

b) Certificate Authority.

c) Communication Authority.

d) Combination Authority

12)Session keys are transmitted after being encrypted by

a) make-shift keys

b) temporary keys

c) master keys

d) section keys

13)The digest created by hash function is normally called?

a) Modification detection Code(MDC)

b) Modify authentication connection

c) Message authentication control

d) Message authentication cipher

14) Full form of HMAC?

a) Hash based Message Authentication Code.

b) Hash based Message Authority Code.

c) Hash based Modification Authorization Code.

d) Hash based Message Automatic Code.

15)Which of the following security services cannot be achieved using the Hash functions?

a) Password Check

b) Data Integrity check

c) Digital Signatures

d) Data retrieval in its original form

16)When a hash function is used to provide message authentication, the hash function value is referred to as

a) Message Field

b) Message Digest

c) Message Score

d) Message Leap

17) A__Trusted third Parties that assigns symmetric key to two Parties?

a. KDC

b. CA

c. KDD

d. both a and c

18)For a client-server authentication, the client requests from the KDC a _____ for access to a specific asset.

a) Ticket

b) local

c) token

d) user

19)What is anomaly detection in IDS?

a. Rules Based.

b. Action based

c. Custom based

d. Stack based.

20)_____ is an attack where the attacker is able to guess together with the sequence number of an in progress communication session & the port number.

a) TCP Spoofing

b) TCP Blind Spoofing

c) IP Spoofing

d) IP Blind Spoofing.