T. Y. B. Sc. I. T. Sem V OLD

Network Security

1. -------- is the breach to authenticity
   A) Access control
   B) Masquerade
   C) Phishing
   D) Fabrication

2. ------ attacks, do not involve any modification to the content of the original message.
   A. Active attack
   B. Passive attack
   C. Denial of Service
   D. Criminal attack.
3. In ------ an attacker sends packet with an incorrect source address.
   A. Packet Spoofing
   B. Packet Sniffing
   C. Phishing
   D. Eavesdropping

4. In ----- substitution cipher technique replaces one block of plain text with another block of cipher text.
   A. Polyalphabetic
   B. Polygram
   C. Homophonic
   D. Mono-Alphabetic

5. -------- works on multiple letters at the same time.
   A. Caesar Cipher
   B. Block Cipher
   C. Hill Cipher
   D. Stream Cipher

6. If the same key is used for encryption and decryption then this mechanism is called as ____.
   A. Asymmetric key cryptography
   B. Symmetric key cryptography
   C. Public key cryptography
   D. Private key cryptography.

7. ------- is a technique that facilitates hiding of message that is to be kept secret inside other messages.
   A. Steganography
   B. Cryptography
   C. Rail Fence
   D. Phishing

8. In ----- attack, attacker does not have any clue about the plain text.
   A. Cipher text only
   B. Known plain text
   C. Chosen plain text

D. Chosen Cipher text

9. In ------ attacker selects a plain text block and tries to look for the encryption of the same in the cipher text.
   A. Cipher text only attacks
   B. Known Plain text attack
   C. Chosen plain text attacks
   D. Chosen cipher text attacks

10. ------means the transforming a single character of the input will alter multiple characters of the output.
    A) Confusion
    B) Diffusion
    C) DES
    D) MD

11. DES consists of 16 steps , each of which is called a -----
    A. Stages
    B. Counters
    C. Rounds
    D. Phases

12. In Expansion permutation the 32 bit Right Plain Text is expanded to ___
    A) 48 bits
    B) 64 bits
    C) 56 bits
    D) 128 bits

13. The output of final permutation is ----- encrypted block.
    A. 32 bit
    B. 16 bit
    C. 56 bit
    D. 64 bit

14. In Advanced Encryption Standard (AES) process each round comprises of ___
    A) 2 sub processes
    B) 4 sub processes
    C) 1 sub processes
    D) 3 Sub processes

15. a -------- issues, Catalogs, renews, and revokes certificates under the management of a policy and administrative control
    A) Certificate authority (ca)
    B) digital certificate
    C) ca manager
    D) root ca

16. A group of software, hardware, people, procedures and policies are known as _____.
    A) Public key infrastructure
    B) Private key infrastructure
    C) Intranet
    D) RA

17. A digital signature needs a(n)_____ system

A) symmetric-key
B) asymmetric-key
C) either (a) or (b)
D) private key

18. In SET process, ------is given to the user for transactions.
A) Pin number
B) Captcha
C) Electronic Wallet
D) ID

19.-------- protocol allows client server applications to communicate across a network to prevent eavesdropping and tampering.
A) Secure Socket Layer protocol
B) Transmission Control Protocol
C) Transport Layer Security
D) File Transfer Protocol.

20. Message Authentication code is also known as Cryptographic____
A) Algorithm
B) Checksum
C) Key
D) Function

21. Digital Signature Algorithm is used for the implementation of ___.
A) DSS
B) Hash
C) Encryption
D) Decryption

22. The identification of each Kerberos principal is its ___
A) Number
B) ID
C) Address
D) Name

23. ____ is a key feature in multi user system.

A) Identification
B) Authorization
C) Authentication
D) Integrity

24. Fabrication causes -------- attack.
A. Denial of service
B. Masquerade
C. Replay attack
D. Alteration

25. --------- software programs did not rely on simple virus signature.

A. First Generation anti virus
B. Second Generation anti virus
C. Third Generation anti virus
D. Fourth Generation anti virus