T.Y.B.Sc. Computer Science

Information and network security

1. DES is an example of _____
   A) Caesar cipher
   B) Block cipher
   C) Stream cipher
   D) Feistel block cipher

2. Vigenere cipher is a ------ substitution technique.
   A) Alphabetic
   B) Arithmetic
   C)Geometric
   D) poly-alphabetic

3. Feistel cipher is based on the principle of ------cipher.
   A) Product
   B) Stream
   C) Block
   D) cryptography

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

5. In PKE, when the key is known to both sender and receiver even if its secret, is known as ___
   A) Asymmetric
   B) Cryptography
   C) Symmetric key cryptography
   D) Caesar cipher
6. In DES , Substitution is called as ___
   A) Diffusion
   B) Transposition
   C) Confusion
   D) Substitution

7. In Expansion permutation the 32 bit RPT is expanded to ___
   A) 48 bits
   B) 64 bits
   C) 56 bits
   D) 128 bits

8. AES is a_____ 128 bit block data encryption technique.
   A) Asymmetric
   B) Session
   C) Symmetric

D) algorithm

9. In cipher block chaining mode before the encryption process ____operation performs between each plain text block and prior cipher text block.

A) XOR
B) OR
C) NOT
D) AND

10. Cipher feedback mode is basically used for ___ .

A) Stream cipher
B) Caesar cipher
C) Asymmetric cryptography
D) Symmetric cryptography

11.___ attack exploits timing variations in operation.

A) Brute force
B) Timing
C) Cipher text attacks
D) Man in middle

12. In digital signature, sender signs a message with its _____ key.

A) Session

B) Public

C) Private

D) Symmetric

13. Nowadays ____ bit key is considered safe.

A) 32

B) 64

C) 128

D) 160

14. Message Authentication code is also known as Cryptographic____

A) Algorithm
B) Checksum
C) Key
D) Function

15. Values received by a hash functions are called as __

A) Message digester
B) Operators
C) Hash1
D) Integers

16. SHA is a group of cryptographic functions intended to maintain data ____
A) Integrity
B) Security
C) Availability
D) Identity

17. Digital signature must be in ___ pattern which depends on message being signed.
A) Byte
B) Bit
C) Vector
D) Pixel

18. In ___ even if the important parts of the network does not operate , the system should work.
A) Decentralization
B) Redundancy
C) Asynchronous
D) Concurrency

19._____ issues and verifies the digital certificates, supports various administrative functions.
A) Certificate Authority
B) Registration Authority
C) Central Directory
D) Central Management System

20. The message digest is appended in __
A) AH
B) Header
C) Trailer
D)Payload

21. IKE framework defines key and____ used to make a secure connection with a peer security gateway.
A) Rules
B) Protocol
C) Algorithms
D) Security

22. Which protocol allows the server and client to authenticate each other using a common encryption algorithms and keys for exchanging of data.
A) TLS Record Protocol
B) TLS Handshake Protocol
C) Transport Layer Security
D) SSL Alert Protocol

23. Which protocol is used by master card and visa for protecting credit card transactions over unprotected networks.
A) Secure Electronic Transaction
B) SSL Alert Protocol
C) TLS Record Protocol
D) Transport Layer Security

24.____ means malicious software.
A) Virus

B) Worm
C) Spyware
D) Malware

25. ___ acts like a guard between your computer and internet.
A) Gateway
B) Scanner
C) Firewall
D) Antivirus