1.Message **________** means privacy that the sender and reciever expect privacy.

A) confidentiality

B) integrity

C) authentication

D) Authorization

Ans: A)confidentiality *

2. Message**_____** means that the data must arrive at the reciever exactly as sent

A) confidentiality

B) integrity

C) authentication

D)Authorization

Ans: B) integrity

3. Message **_______** means that the receiver is ensured that the message message is coming from the indended sender not an imposter.

A)confidentiality

B)integrity

C)authentication

D) Authorization

Ans:C) authentication

4.**__________means that a sender must not be able to deny sending a message that he sent.**

A)Confidentiality

B)Integrity

C)Authentication

D)Nonrepudiation

Ans: D) Nonrepudiation

5.A(n)________________can be used to preserve the integrity of a document or a message.

A)message digest

B)message summary

C)encrypted message

D)ENCRYPTION

Ans:A) message digest

6.A(n)______________function creates a message digest out of a message.

A. encryption

B. decryption

C. hash

D.integrity

Ans: C) hash

7.A hash function must meet_____________________criteria.

A)two

B)three

C)four

D)ten

Ans: B)three

8.Password-based authentication can be divided into two broad categories:_____and ________

A)fixed; variable

B)time-stamped; fixed

C)fixed; one-time

D)none of the above

Ans: C) fixed; one-time

9._creates a secret key only between a member and the center.

A. CA

B. KDC

C. KDD

D. CD

Ans:B) KDC

10.The secret key between members needs to be created as a ________ key when two members contact KDC.

A.public

B.session

C.complimentary

D.private

Ans: B) session

11. is a popular session key creator protocol that requires an authentica ion server and a ticket-granting server.

A)KDC

B)Kerberos

C)CA

D)CD

Ans:A) KDC

12.A(n)___________is a hierarchical system that answers queries about key certification.

A)KDC

B)PKI

C)CA

D)CD

Ans:C) CA

13.Firewalls are to protect against

(A) Virus Attacks

(B) Fire Attacks

(C) Data Driven Attacks

(D) Unauthorized Attacks

Ans:D) Unauthorized Attacks

14.The_________criterion ensures that we cannot find two messages that hash to the same digest

A)one-wayness

B)weak-collision-resistance

C)strong-collision-resistance

D) Keyless

Ans: B)weak-collision-resistance

15.________________________ is a term used in cryptography that refers to a message before encryption or after decryption.

A)Cipher text

B)Plain text

C)Plain script

D) Original text

Ans: A)Cipher text

16. The ________ is encrypted text

A) cipher text

B)cipher scricpt

C)secret text

D) secret script

Ans: C)secret text

17. ________________________ ensures that information are in a format that is true and correct to its original purposes.

A)Availability

B)Confidentiality

C)Cryptography

D) Integrity

Ans: A)Availability

18. ______________________ ensures that information and resources are available to those who need them.

A)Availability

B) Confidentiality

C)Cryptography

D)Integrity

Ans: D) Integrity

19. ________________________ is the process of identifying an individual, usually based on a username and password.

A)Authentication

B) Authorization

C)integrity

D) crytography

Ans: A)Authentication

20. ____________________ is the process of giving individuals access to system objects based on their identity.

A) Authentication

B)Authorization

C) key

D)Confidentiality

Ans: B)Authorization

21. In symmetric-key cryptography, the key locks and unlocks the box is

A. Same

B. shared

C. private

D. Public

Ans:A) Same

22. The ciphers of today are called round ciphers because they involve

A.Single Round

B.Double Rounds

C.Multiple Round

D.Round about

Ans: C.Multiple Round

23.Symmetric-key cryptography started thousands of years ago when people needed to exchange

A.Files

B.Packets

C.Secrets

D.Transmission

Ans:C.Secrets

24.The Advanced Encryption Standard (AES) was designed

A. National Institute of Standards and Technology

B. IBM

C. HP

D. Intel

Ans:A National Institute of Standards and Technology

25.The Mobile Application Protocol (MAP) typically runs on top of which protocol ?

A. SNMP (Simple Network Management Protocol)

B. SMTP (Simple Mail Transfer Protocol)

C. SS7 (Signalling System 7)

D. HTTP (Hyper Text Transfer Protocol)

Ans:C. SS7 (Signalling System 7)

26.If a packet arrive with an M-bit value is '1' and a fragmentation offset value '0', then it is ______ fragment.

A. First

B. Middle

C. Last

D. Four

Ans:A) First

27.The design issue of Datalink Layer in OSI Reference Model is

A. Framing

B. Representation of bits

C. Synchronization of bits

D. Connection control

Ans:A) Framing

28.Data Encryption Techniques are particularly used for ________.

A. protecting data in Data Communication System

B. reduce Storage Space Requirement

C. enhances Data Integrity

D. decreases Data Integrity

Ans:A) protecting data in Data Communication System

29.An example of a layer that is absent in broadcast networks is:

A. Physical layer

B. Presentation layer

C. Network layer

Application layer

Ans:C. Network layer

30.Encryption and Decryption is the responsibility of ___ Layer.

A. Physical

B. Network

C. Application

D. Datalink

Ans:C: Application

31.The VLF and LF bauds use propagation for communication

A.Ground

B.Sky

C.Line of sight

D.Space

Ans:A) .Ground

32. The start and stop bits are used in serial communication for

A. error detection

B. error correction

C. Synchronization

D. slowing down the communication

Ans:C Synchronization

33. ____________ is a type of transmission impairment in which the Signal looses strength due to The resistance of the transmission medium.

A. Attenuation

B. Distortion

C. Noise

D. Decible

Ans: A) Attenuation

34. _________________ is a bit-oriented protocol for communication over point-to-point and multi-point links .

A. Stop-and-wait

B. HDLC

C. Sliding window

D. Go-back-N

Ans:A) Stop-and-wait

35. In substitution, a character in the plaintext is always changed to the same character in the ciphertext, regardless of its position in the text.

A. polyalphabetic

B. mono alphabetic

C. Transpositional

D. multialphabetic

Ans: B) mono alphabetic

36. Which of the following is not associated with the session layer ?

A. Dialog control

B. Token management

C. Semantics of the information transmitted

D. Synchronization

Ans: C) Semantics of the information transmitted

37. What is the size of the 'total length' field in IPv4 datagram ?

A. 4 bits

B. 8 bits

C. 16 bits

D. 32 bits

Ans:C) 16 bits

38. The process of dividing an analog signal into a string of discrete outputs, each of constant amplitude, is called :

A. Strobing

B. Amplification

C. Conditioning

D. Quantization

Ans: d) Quantization

39.Which transmission technique guarantees that data packets will be received by the receiver in the same order in which they were sent by the sender.

A.Broadcasting

B.Unicasting

C.Packet switching

D.Circuit switching

Ans:d) Circuit switching

40.Which of the following control fields in TCP header is used to specify whether the sender has no more data to transmit?

A. FIN

B. RST

C. SYN

D. PSH

Ans:A) FIN

41.Which are the two modes of IP security?

A.Transport and certificate

B.Transport and tunnel

C.Certificate and tunnel

D.Preshared and transport

Ans: B) .Transport and tunnel