Set 1: Wireless Security MCQS – FAQ by GRE

1. Which of these is the anticipation of unauthorized access, data or break to computers by means of wireless networks?
A. Wireless security
[✓ B. Wireless access]
C. Wired device apps
D. Wired Security
E. Both A & B
F. None of these

B

2. Which of the following has the strongest wireless security?
A. WPA
B. WEP
[✓ C. WPA3]
D. WPA2
E. Both A & B
F. None of these
3. Which of the following is has the worst security encryption standard?
A. WPA
B. WPA2
C. WPA3
[✓ D. WEP]
E. Both C & D
F. None of these
4. Which is an old IEEE 802.11 standard that was released in 1999?
[✓ A. WEP]
B. WPA
C. WPA2
D. WPA3
E. Both A & B
F. None of these
5. Central node of 802.11 wireless operations is ______________
[✓ A. Access Point]
B. WPA
C. Access Port
D. WAP
E. Both A & B
F. None of these
6. AP stands for
A. Access Port
[✓ B. Access Point]
C. Accessing Port
D. Access Position
E. Both A & B
F. None of these
7. ____________ is similar to AP from 802.11 and is used by mobile operators for offering signal coverage.

[✓ A.] Base Transmitter Station ✓
B. Base Signal Station
C. Transceiver Station
D. Base Transceiver Station
E. Both C & D
F. None of these
8. BTS is abbreviated as_______________________________
A. Base Transceiver Server
[✓ B.] Base Transceiver Station
C. Base Transmitter Station
D. Basement Transceiver Server
E. Both A & B
F. None of these
9. How many types of wireless authentication modes? : open, individual enterprise
A. 5
[✓ B.] 3 B
C. 2
D. 4
E. Both A & B
F. None of these
10. When a user authenticates to an AP, both go in the path of four-step authentication progression which is known as _______________
[✓ A.] 4-way handshake ✓
B. AP-handshaking
C. Wireless handshaking
D. 4-way connection
E. Both A & B
F. None of these

Set 2: Wireless Security MCQS – FAQ by GAT Subject NTS Test

11. WPS is abbreviated as ______________________________
A. WiFi Protocol Setup
[✓ B.] Wireless Protected Setup ✓
C. WiFi Protected Setup
D. WiFi Protected System
E. Both A & B
F. None of these

12. It is to use encryption standard such as WPA2 or WPA3 as they are more secure and strong. ✓
A. False
[✓ B.] True
C. Both A & B
D. None of these
13. Cryptosystem with asymmetric-key has its own _______________ with confidentiality.
A. Data
[✓ B.] Entities :
C. Translator
D. Problems
E. Both C& D
F. None of these
14. Message digestion length of SHA-1 is __________ B?

C. 820 bits ✗

[✓ D. 160 bits] ✓

E. Both C& D

F. None of these

15. _____________ is a service beyond message authentication?

A. Message Splashing

B. Message Sending

[✓ C. Message Integrity] ✓

D. Message Confidentiality

E. Both B & C

F. None of these

16. The transmitted message must make sense only to intended ____________, in message confidentiality.

A. Sender

[✓ B. Receiver] ✓

C. Translator

D. Modulor

E. Both A & B

F. None of these

17. Hash functions guarantee message integrity and that the message has not been _________.

A. Over view

B. Replaced

C. Violated

D. Changed

[✓ E. Both C & D]

F. None of these

18. _____________ is needed by a digital signature.

A. Public-key system

B. Private-key system

C. Shared-key system

[✓ D. Both A & B]

E. All of them

F. None of these

19. Using a _______________ is also another way to preserve the integrity of the document.

A. Biometric ✗

B. Eye-Rays

C. X-Rays

[✓ D. Finger Print]

E. Both C & D

F. None of these

20. How many times do a session symmetric key between the two parties is used?

[✓ A. Multiple times]

B. Only once

C. Conditions dependant

D. Twice

E. Both C & D

F. None of these

\

21. ___________ is not provided by encryption and decryption.

A. Integrity

B. Privacy

[✓ D. Both A & B]
E. All of the above
F. None of these

22. MAC is abbreviated as
A. Message arbitrary connection
[✓ B. Message authentication code]
C. Message authentication cipher
D. Message authentication control
E. Both B & C
F. None of these

23. Message confidentiality uses ___________
A. Cipher
B. Symmetric-Key
C. Asymmetric-Key
D. Cipher Text
[✓ E. Both C & D]
F. None of these

24. Both document and fingerprint are ___________ to preserve integrity of a document.
A. Not needed
[✓ B. Needed]
C. Not Used
D. Unimportant
E. Both A & B
F. None of these

25. Data must arrive exactly as it was sent to receiver from sender, is called ____________.
A. Message Sending
B. Message Splashing
[✓ C. Message Integrity] ✓
D. Message Confidentiality
E. Both C & D
F. None of these

26. Encryption is done at sender site and decryption is done at ____________
[✓ A. Receiver site] ✓
B. Sender Site
C. Conferencing
D. Site
E. Both A & B
F. None of these

27. EAP is abbreviated as
A. Embedded Authentication Protocol
B. Embedded Application Protocol
C. Extended Application Protocol
[✓ D. Extensible Authentication Protocol] ✓
E. Both C & D
F. None of these

28. Is TKIP an access control protocol? ?
[✓ A. False]
B. True
C. Can't say
D. May be
E. Both A & B

28

29. AAA key (Authentication, Authorization and Accounting Key) is also known as

A. pairwise transient key

[✓ B. master session key] ✓

C. key confirmation key

D. pre-shared key

E. Both B & C

F. None of these

30. Wi-Fi is abbreviated as

A. Wireless FLAN

B. Wireless LAN

[✓ C. Wireless Fidelity]

D. Both B & C

E. None of these

Set 4: Wireless Security MCQS – FAQ by Network Administrator Job Test

31. Wired networks are more vulnerable to jamming and eavesdropping then wireless networks.

[✓ A. False]

B. True

cant attack wired netwoeks with jamming

C. May be

D. Can’t say

E. Both A & B

F. None of these

32. In which year wireless communication started?

A. 1869

B. 1879

C. 1885

D. 1895

E. Both C & D

[✓ F. None of these]

33. If we lack a central point of control, which type of wireless network threat it would be?

A. Non-Traditional Networks

B. Identity Theft

C. Man in the middle attack

[✓ D. Ad Hoc Networks]

E. Both C & D

F. None of these

34. Scamming/fake access points are created to access data such as credit card information, which type of threats is this?

A. Malicious Association

B. Man in the middle attack

C. Network Injection

D. Identity Theft

[✓ E. Both A & B]

F. None of these

35. To affect routers and switches false reconfiguration commands are used, which type of threats is this?

A. Malicious Association

[✓ B. Network Injection]

C. Denial Of Service

D. Man in the middle attack

E. Both A & B

36. When there is an intermediate between the communications without the knowledge of the communicators, which type of threats is this?

A. Network Injection

B. Malicious Association

C. Accidental Association

[✓ D. Man in the middle attack]

E. Both A & B

F. None of these

37. SSID is abbreviated as

[✓ A. Service Set Independent Device]

B. Secure Set Identifier

C. Secure Set Independent Device

D. Secure Service Identifier

E. Both A & B

F. None of these

38. Which of the following is not a legitimate Signal-Hiding Technique? hide wireless network (physical layer)

[✓ A. installing the wireless access point away from exteriors of the building]

B. using directional antennas and signal shielding techniques transmit in a way we want

C. reducing the signal strength to the lowest level such that it still provides requisite coverage cover a area not all

D. Both A & B

E. None of these

~~39. Mobile Device security has 3 categories. Which of the following is not a Mobile Device security category?~~

~~A. Traffic security~~

~~B. Device security~~

~~C. Range security~~

~~D. Barrier security~~

~~E. Both A & B~~

~~F. None of these~~

~~40. Many companies prohibited the installation of third-party applications on the company's hardware devices. Which Mobile Device security category implements this?~~

~~A. Traffic security~~

~~B. Device security~~

~~C. Barrier security~~

~~D. Both A & B~~

~~E. None of these~~

41. VPN is abbreviated as

[✓ A. Virtual Private Network]

B. Visual Performance Node

C. Virtual Post Network

D. Virtual Post Node

E. Both A & B

F. None of these

42. Wireless Ethernet 802.11a is also known as

A. Wi-Fi6

B. Wi-Fi5

C. Wi-Fi4

[✓ D. Wi-Fi]

E. Both A & B

F. None of these

~~43. In IEEE 802.11, MSDU is abbreviated as~~

~~[✓ A. Multiframe service datagram usage]~~

~~B. MAC server device usage~~

~~C. MAC service data unit.~~

~~D. Main server data user~~

~~E. Both C & D~~

~~F. None of these~~

44. In which layer frequency band is defined and wireless signals are encoded?

A. Medium Access Layer

B. Physical Layer

[✓ C. Logic Link Control Layer] = link layer (OSI)

D. Both B & C

E. None of these

~~45. The right sequence of the MAC header is~~

~~[✓ A. Source MAC Address, Destination MAC Address, MAC Control]~~

~~B. MAC Control, Destination MAC Address, Source MAC Address~~

~~C. Destination MAC Address, Source MAC Address, MAC Control~~

~~D. Both A & B~~

~~E. None of these~~

46. Does MAC trailer have CRC in its components?

A. Can’t say

[✓ B. False]

C. True

D. May be

E. None of these

47. Which layer is responsible for keeping track of all the transmitted and received frames?

[✓ A. Logic Link Control Layer]

B. Medium Access Layer

C. Physical Layer

D. Both C & D

E. None of these

48. All communications are done through APs in IBSS system.

A. False

[✓ B. True]

C. Can’t say

D. May be

E. None of these

49. Which security algorithm was defined for the IEEE 802.11?

A. RSN

[✓ B. WEP]

C. SSL

[✓ D. WPA]

E. Both A & B

F. None of these

50. 802.11i’s final form is known as

A. Wi-Fi Protected Access

B. Wired Equivalency Privacy

D. Both A & B
E. None of these

51. In TKIP, the size of the temporal key is?
A. 512 bits
B. 256 bits
C. 128 bits
D. 64 bits
E. Both B & C
F. None of these

52. In WEP, what is the valid size of Group Temporal Key?
A. 512 bits
B. 128 bits
C. 80 bits
D. 40 bits
E. Both C & D
F. None of these

53. ________ is the size of message integrity code key?
A. 512 bits
B. 128 bits
C. 64 bits
D. 256 bits
E. Both C & D
F. None of these

54. ___________ is not a traffic control key.
A. MIC Key
B. WEP Key
C. TK
D. GTK
E. Both C & D
F. None of these