

COMPUTER SECURITY

Question Bank

Helping Others Have Special taste

Questions

1) Is an ancient art and science of secret writing.

- A – **Cryptography**
- B – Encryption
- C – Decryption
- D – None of the above

2) Measures to protect data during their transmission.

- A – Computer Security
- B – **Network Security**
- C – Internet Security
- D – None of the above

3) Measures to protect data during their transmission over a collection of interconnected networks.

- A – Computer Security
- B – Network Security
- C – **Internet Security**
- D – None of the above

4) Generic name for the collection of tools designed to protect data.

- A – **Computer Security**
- B – Network Security
- C – Internet Security
- D – None of the above

5) Ensuring that no one can read the message except that the intended receiver.

- | | |
|----------------------------|-----------------------|
| A – Integrity | B – Availability |
| C – Confidentiality | D – None of the above |

6) Assuring the receiver that the received message has not been altered in any way from the original.

A – Integrity

B – Availability

C – Confidentiality

D – None of the above

7) Ensuring timely and reliable access to and use of information.

A – Integrity

B – Availability

C – Confidentiality

D – None of the above

8) Guarding against improper information modification or destruction including ensuring information nonrepudiation and authenticity.

A – Integrity

B – Availability

C – Confidentiality

D – None of the above

9) Preserving authorized restrictions on information access and disclosure including means for protecting personal privacy and proprietary information.

A – Integrity

B – Availability

C – Confidentiality

D – None of the above

10) A loss of is the disruption of access to or use of information or an information system.

A – Integrity

B – Availability

C – Confidentiality

D – None of the above

11) A loss of is the unauthorized disclosure of information.

- A – Integrity
- B – Availability
- C – Confidentiality**
- D – None of the above

12) A loss of is the unauthorized modification or destruction of information.

- A – Integrity**
- B – Availability
- C – Confidentiality
- D – None of the above

13) Ensures that computer related assets are accessed only by authorized parties.

- A – Integrity
- B – Availability
- C – Confidentiality**
- D – None of the above

14) Assets can be modified only by authorized parties or only in authorized way.

- A – Integrity**
- B – Availability
- C – Confidentiality
- D – None of the above

15) Assets are accessible to authorized parties at appropriate time.

- A – Integrity
- B – Availability**
- C – Confidentiality
- D – None of the above

16) OSI stands for

- A – Open System Interpreter
- B – Open Secure Interpreter
- C – Open Secure Interconnect
- D – Open System Interconnect

17) The OSI security architecture focuses on

- A – Security mechanism
- B – Security service
- C – Security attack
- D – All of the above

18) A process that is designed to detect, prevent, or recover from a security attack.

- A – Security mechanism
- B – Security service
- C – Security attack
- D – All of the above

19) A process or communication service that enhance the security of the data processing systems and the information transfers of an organization.

- A – Security mechanism
- B – Security service
- C – Security attack
- D – All of the above

20) Make use of one or more security mechanisms to provide the service.

- A – Security mechanism
- B – Security service
- C – Security attack
- D – All of the above

- 21) Any action that compromises the security of information owned by an information.
- A – Security mechanism
 - B – Security service
 - C – Security attack
 - D – All of the above
- 22)..... is about how to prevent attacks or failing that, to detect attacks on information-based systems.
- A – Security attack
 - B – Information security
 - C – Security mechanism
 - D – None of the above
- 23) A / An..... attack attempts to learn or make use of information from the system but does not affect system resources.
- A – Active
 - B – Passive
 - C – Negative
 - D – None of the above
- 24) A/An attack attempts to alter system resources or affect their operation.
- A – Active
 - B – Passive
 - C – Negative
 - D – None of the above
- 25) Is the scrambled message produced as output.
- A – Plaintext
 - B – Ciphertext
 - C – Security key
 - D – None of the above

26)The original message or data.

- A – Plaintext
- B – Ciphertext
- C – Security key
- D – None of the above

27)Is a value independent of the original message and of the algorithm.

- A – Plaintext
- B – Ciphertext
- C – Security key
- D – None of the above

28)Is a mathematical procedure for performing encryption on data.

- A – Security key
- B – Decryption algorithm
- C – Encryption algorithm
- D – None of the above

29)Is a mathematical procedure for performing decryption on data.

- A – Security key
- B – Decryption algorithm
- C – Encryption algorithm
- D – None of the above

30)Which type of keys that is more secure and cause slow processing.

- A – Shorter keys
- B – longer keys
- C – Single use key
- D – Multi use key

31)Which type of keys that is less secure and faster in processing.

- A – Shorter keys
- B – longer keys
- C – Single use key
- D – Multi use key

32)Used to encrypt one message only.

- A – Shorter keys
- B – longer keys
- C – Single use key**
- D – Multi use key

33)Used to encrypt multiple messages.

- A – Shorter keys
- B – longer keys
- C – Single use key
- D – Multi use key**

34)Symmetric encryption best known as

- A – Public key algorithm
- B – Shared secret key algorithm**
- C – long key algorithm
- D – None of the above

**35)In symmetric encryption, the sender and receiver must share a
Key.**

- A – Secret**
- B – Public
- C – Encrypted
- D – None of the above

36)In symmetric encryption, the usual key length is bits.

- A – 512 – 4094
- B – 512 – 4096
- C – 80 – 256**
- D – 80 – 254

- 37) **A cipher is a symmetric key cipher where plaintext digits are combined with pseudorandom cipher digit stream.**
- A – Stream**
 - B – Block
 - C – Line
 - D – None of the above
- 38) **A cipher is a symmetric key cipher in which a cryptographic key and algorithm are applied to a block of data at one as a group rather than to one bit at a time.**
- A – Stream
 - B – Block**
 - C – Line
 - D – None of the above
- 39) **Asymmetric encryption known as**
- A – Public key algorithm**
 - B – Shared secret key algorithm
 - C – long key algorithm
 - D – None of the above
- 40) **In asymmetric encryption, the usual key length is bits.**
- A – 512 – 4094
 - B – 512 – 4096**
 - C – 80 – 256
 - D – 80 – 254
- 41) **the term referring to the wide study of secret writing.**
- A – Cryptanalysis
 - B – Cryptography
 - C – Cryptology**
 - D – None of the above

42) the science of analysing and breaking encryption schemes.

- A – Cryptanalysis
- B – Cryptography
- C – Cryptology
- D – None of the above

43) ____ is the process of communicating confidential information in an unreadable format between legitimate users?

- A - Cryptography
- B - Symmentricity
- C - Asymmenticity
- D - All the above

44) Which are the ends does cryptography process takes place?

- A - Transmitter
- B - Receiver
- C - Channel
- D - Both a and b

45) We use Cryptography term to transforming messages to make them secure and immune to

- A - Change
- B - Idle
- C - Attacks
- D – Defend

46) Cryptography, a word with Greek origins, means

- A - Corrupting Data
- B - Secret Writing**
- C - Open Writing
- D - Closed Writing

47) Cryptography can provide

- A - entity authentication
- B - nonrepudiation of messages
- C - confidentiality**
- D - All of them**

48) In computer security, means that computer system assets can be modified only by authorized parties.

- A - Confidentiality
- B - Integrity**
- C - Availability
- D - Authenticity

49) Data encryption is primarily used to ensure confidentiality

- A - true**
- B - false

50) Identify the term which denotes that only authorized users are capable of accessing the information

- | | |
|----------------------------|------------------|
| A - Confidentiality | B - Integrity |
| C - Availability | D - Authenticity |

51) Identify the term which denotes the violation of principle if the computer is no more accessible

A - Confidentiality

B - Integrity

C - Availability

D - Authenticity



52) means the security of data from tampering by unidentified users.

A - Confidentiality

B - Integrity

C - Authentication

D - Non-repudiation

53) What is the CIA Triad ?

A - A branch of the Central Intelligence Agency

B - Cryptography, Information, Analysis

C - Confidentiality, Information, Availability

D - Confidentiality, Integrity, Availability

54) According to the CIA Triad, which of the below-mentioned element is not considered in the triad?

A - Integrity

B - Authenticity

C - Availability

D - Confidentiality

55) Which of the following is an objective of network security?

A - Confidentiality

B - Integrity

C - Availability

D - All of the Above

56) This is the model designed for guiding the policies of Information security within a company, firm or organization. What is “this” referred to here?

- A - Confidentiality
- B - Non-repudiation
- C - CIA Triad**
- D - Authenticity

57) When you use the word _____ it means you are protecting your data from getting disclosed.

- A - Confidentiality**
- B - Integrity
- C - Authentication
- D - Availability**

58) Data _____ is used to ensure confidentiality.

- A - Encryption**
- B - Locking
- C - Deleting
- D - Backup

59) The message before being transformed, is

- A - Simple Text
- B - Cipher Text
- C - Empty Text
- D - plain text**

60) What is transformed using cipher algorithms?

- A - plain text**
- B - complex text
- C - scalar text
- D - none

61) In cryptography, what is cipher?

- A - algorithm for performing encryption and decryption
- B - encrypted message
- C - both algorithm for performing encryption and decryption and encrypted message
- D - decrypted message

62) 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

63) Cryptanalysis is used _____

- A - to find some insecurity in a cryptographic scheme
- B - to increase the speed
- C - to encrypt the data
- D - to make new ciphers

64) Which of the following term defines the string of char that assist during encryption and decryption of confidential message?

- A - Cipher
- B - Plain text
- C - Key
- D - All the above

65) Which of the following are the components of crypto system?

- A - Plain text
- B - Cipher text
- C - Keys
- D - All the above

66) Which of the following is an encryption key of assymetric system?

- A - Public**
- B - Private
- C - Both a and b
- D - Zero key

67) Which of the following is an decryption key of assymetric system?

- A - Public
- B - Private**
- C - Both a and b
- D - Zero key

68) Symmetric key ciphers are deployed using?

- A - Stream cipher
- B - Block cipher
- C - Bit cipher
- D - Both a and b**

Answers

Question	Answer
1	A
2	B
3	C
4	A
5	C
6	A
7	B
8	A
9	C
10	B
11	C
12	A
13	C
14	A
15	B
16	D
17	D
18	A
19	B
20	B
21	C
22	B
23	B

Lecture-3

24	A
25	B
26	A
27	C
28	C
29	B
30	B
31	A
32	C
33	D
34	B
35	A
36	C
37	A
38	B
39	A
40	B
41	C
42	A
43	A
44	D
45	C
46	B
47	D
48	B
49	A
50	C
51	C
52	B
53	D

Lecture-3

54	B
55	D
56	C
57	A
58	A
59	D
60	A
61	A
62	B
63	A
64	C
65	D
66	A
67	B
68	D

We Hope we could Help You

Please leave us your feedback

Your Feedback Here [Feedback](#)