1. _____ is the science to make them secure and immune to attacks.
a) Cryptography
b) Cryptoanalysis
c) both (a) or (b)
d) neither (a) nor (b)

2 A combination of an encryption algorithm and a decryption algorithm is called a _____.

A. cipher

B. secret

C. key

D. none of the above

3. _____ ciphers can be categorized into two broad categories:

monoalphabetic and polyalphabetic.

A. Substitution

B. Transposition

C. both (a) or (b)

D. neither (a) nor (b)

4. A _____ is a keyless transposition cipher with N inputs and M outputs that uses a table to define the relationship between the input stream and the output stream

a. S-box

b. P-box

c. T-box

D. none of the above

5. DES has an initial and final permutation block and rounds

A. 14

B. 15

C. 16

D. 18

6. ECB and CBC are _____ ciphers

a. block

b. stream

c. field

d. none of the above

7. The ------- method provides a one-time session key for two parties

a. Diffie-Hellman

b. RSA

c. DES

d. AES

8. Message _____means that the receiver is ensured that the message is coming from the intended sender, not an imposter.

a. confidentiality

b. integrity

c. authentication

d. none of the above

9. Digital signature provides

a. authentication

b. nonrepudiation

c. both (a) and (b)

d. neither (a) nor (b)

10. A(n) _____ is a trusted third party that assigns a symmetric key to two parties.

A. KDC

B. CA

C. KDD

D. none of the above

11. Intrusion is action or process that compromises Authentication, integrity, availability of system

A. force fully

B. With Permission

C. Without Permission

D . Both A and C

12. Intruder is ____.

A. Action

B. User

C System

D. Data

13. Misfeasor intruder is normally?

A. Insider

B. Outsider

C. Both A and B

D. Middle

15. What are the different ways to classify IDS?

A. Statistical anomaly detection

B. Rule based detection

C. Both A and B

D. Stack based.

16. What is anomaly detection in IDS?

A. Rules Based.

B. Action based

C. Custom based

D. Stack based.

17. In which approach an expert system is used to search for suspicious behavior of user?

A. Anomaly detection.

B. Penetration identification.

C. Profile based

D. Machine based.

18. Is Auditing Records keeping the Track of ongoing?

A. Activity in the system.

B. Function in system.

C. Variable in System.

d. Method in system

19. IDS stand for?

A. Information Detection System

B. Intrusion Detection System

C. Institute Detection System

D. Image Detection System

20. Connection authentication is offered for ensuring that the remote host has the likely Internet Protocol (IP) _____ & _____

a) address, name

b) address, location

c) network, name

d) network, location

21. Full form of SSL is __?

a) Secure Socket Layer

b) Series Socket Layer

c) System Security Layer

d) Spoofing Socket Layer.

22. Which Protocols Design to create sessions between client and server?

a) Handshake

b) FTP

c) Alert

d) UDP.

23. Which protocol is used to transmit error, bad records, system Negotiation failure alerts to the peer entity?

a) Alert Protocol

b) Handshake Protocol

c) Upper-layer Protocol

d) Change Cipher Spec Protocol

24. Which protocol is used for the purpose of reproducing the pending state into the Present state?

a) Alert Protocol

b) Handshake Protocol

c) Upper-Layer Protocol

d) Change Cipher Spec Protocol

25. Secure Electronic Transaction Protocol used for?

a) Credit Card payment.

b) Cheque payment.

c) Cash Payment

d) Payment of small amount for internet Service

26. Full form of “CA” in term of SET Protocols?

a) Chartered Accountant.

b) Certificate Authority.

c) Communication Authority.

d) Combination Assurances

27. Authority who is trusted to provide public key Certificate to Merchant, Card holder and Payment gateway?

a) Serial Authority.

b) Certificate Authority.

c) Communication Authority.

d) Combination Authority

28.Which of them is not a wireless attack?

a) Eavesdropping

b) MAC Spoofing

c) Wireless Hijacking

d) Phishing

29. An attempt to harm, damage or cause threat to a system or network is broadly termed as _____

a) Cyber-crime

b) Cyber Attack

c) System hijacking

d) Digital crime

30. _____ is the art & science of cracking the cipher-text without knowing the key.

a) Cracking

b) Cryptanalysis

c) Cryptography

d) Crypto-hacking

31. The process of disguising plaintext in such a way that its substance gets hidden (into what is known as cipher-text) is called _____

a) cryptanalysis

b) decryption

c) reverse engineering

d) encryption

33. Which of the following is not the primary objective of cryptography?

a) Confidentiality

b) Data Integrity

c) Data Redundancy

d) Authentication

34. _____ is the mathematical procedure or algorithm which produces a cipher-text for any specified plaintext.

a) Encryption Algorithm

b) Decryption Algorithm

c) Hashing Algorithm

d) Tuning Algorithm

35. In _____ 2 different keys are implemented for encrypting as well as decrypting that particular information.

a) Symmetric Key Encryption

b) Asymmetric Key Encryption

c) Asymmetric Key Decryption

d) Hash-based Key Encryption

36. _____at first, a key table is produced. That key table is a 5 by 5 grid of alphabets which operates as the key to encrypt the plaintext.

a) Rolling Cipher

b) Shift Cipher

c) Playfair Cipher

d) Block Cipher

37. In _____ a sequence of actions is carried out on this block after a block of plain-text bits is chosen for generating a block of cipher-text bits.

a) Block Cipher

b) One-time pad

c) Hash functions

d) Vigenere Cipher

38.The DES Algorithm Cipher System consists of _____rounds (iterations) each with a round key

a) 12

b) 18

c) 9

d) 16

39. The DES algorithm has a key length of

a) 128 Bits

b) 32 Bits

c) 64 Bits

d) 16 Bits

40. Which of the following is not a principle of data security?

a)Data Confidentiality

b)Data Integrity

c)Authentication

d)Certification

41. In which attack one entity pretends to be a different entity?

a) Masquerade attack

b) Modification of messages attack

c) Repudiation

d) Replay