Selected Topics (Encryption)

1. “Who is authorized to use data?”, this is known as _____

   a) Confidentiality
   b) Integrity
   c) Availability
   d) Encryption

2. “Is data good?” , this is known as_____

   a) Confidentiality
   b) Integrity
   c) Availability
   d) Encryption

3. “Can access data whenever need it?” , this is known as_____

   a) Confidentiality
   b) Integrity
   c) Availability
   d) Encryption

4. _____ is the avoidance of the unauthorized disclosure of information.

   a) Confidentiality
   b) Integrity
   c) Availability
   d) Encryption

5. The transformation of information using a secret, called an encryption key. This concept is called _____

   a) Authentication
   b) Encryption
   c) Vulnerability
   d) Threat

6. The determination of the identity or role that someone has. This is called ___

   a) Authentication
   b) Authorization

c) Encryption
d) Vulnerability

7. The determination if a person or system is allowed access to resources, based on an access control policy(determines what resources a user can access). This concept is called _____

a) Authentication
b) Authorization
c) Encryption
d) Vulnerability

8. The property that information has not be altered in an unauthorized way.

a) Confidentiality
b) Integrity
c) Availability
d) Encryption

9. _____ is the one who exploit any available mean of hacking to hack a system.

a) Intruder
b) Cipher
c) Vulnerability
d) Threat

10. _____ is a weakness in the security system.

a) Vulnerability
b) Threat
c) Encryption
d) Confidentiality

11. _____ is a set of circumstances that has the potential to cause harm or loss

a) Vulnerability
b) Threat
c) Encryption
d) Confidentiality

12. _____ is the interception of information intended for someone else during its transmission over a communication channel.

a) Eavesdropping
b) Alteration
c) Masquerading
d) Repudiation

13._____ is the denial of a commitment or data receipt.

a) Eavesdropping
b) Alteration
c) Masquerading
d) Repudiation

14._____ is unauthorized modification of information.

a) Eavesdropping
b) Alteration
c) Masquerading
d) Repudiation

15._____ is the fabrication of information that is purported to be from someone who is not actually the author.

a) Eavesdropping
b) Alteration
c) Masquerading
d) Repudiation

16. The _____ encryption is encryption with a single key to both sender and receiver.

a) Symmetric
b) Asymmetric
c) Interruption
d) Interception

17.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

18.Type of attack that is used in Alteration is passive attack

a) True
b) False

19. If the sender and receiver use different keys, the system is referred to as conventional cipher system

a) True
b) False

20. _____ is original message

a) Plaintext
b) Ciphertext
c) Private text
d) None

21. _____ is study of encryption principles/methods.

a) Cryptography
b) Cryptanalysis
c) Cryptology
d) Cipher

22. _____ is study of principles/ methods of deciphering ciphertext without knowing key

e) Cryptography
f) Cryptanalysis
g) Cryptology
h) Cipher

23. “meet” , Encryption of this word with Caesar Cipher is _____

a) MEET
b) OFFU
c) WIIX
d) PHHW

24. In brute force attack, on average half of all possible keys must be tried to achieve success.

a) True
b) False

25. What is the meaning of cipher in cryptography?

a) an algorithm that performs encryption
b) an algorithm that generates a secret code
c) an algorithm that performs encryption or decryption
d) a secret code

26.2. Which of the following is a type of traditional (classical)cipher?

a) transportation cipher
b) transposition cipher
c) transforming cipher
d) vigenere cipher

27. Which of the following is a type of substitution cipher?

a) Mono alphabetic cipher
b) transposition cipher
c) transportation cipher
d) transforming cipher

28. The simplest monoalphabetic cipher is the ____

a) Auto key cipher
b) Hill cipher
c) Playfair cipher
d) Additive cipher

29. Playfair cipher is an example of _____

a) mono-alphabetic cipher
b) poly-alphabetic cipher
c) transposition cipher
d) additive cipher

30. What will be the plain text corresponding to cipher text “BPKYFS” if playfair cipher is used with keyword as “SECRET” (assuming j is combined with i)?

a) INDIAN
b) WORLD
c) DOLLAR
d) HELLO

31. What will be the ciphered text if the string “SANFOUNDRY” is given as input to the code of playfair cipher with keyword as “SECRET” (assuming j is combined with i)?

a) ZHQAPNPAFR
b) AHQAPNPAFR
c) HAQAPNPAFR
d) QHAAPNPAFR

32. The key in vigenere cipher must be less than or equal to the size of the message

a) True
b) False

33. What will be the plain text corresponding to cipher text “PROTO” if vigenere cipher is used with keyword as “HELLO”?

a) SANFOUNDRY
b) WORLD
c) INDIA
d) AMERICA

34. What will be the ciphered text if the string “SANFOUNDRY” is given as input to the code of vigenere cipher with keyword as “HELLO”?

a) UEWIIDKLL
b) ZEYQCOCM
c) ZEYQCBROCM
d) ZEYQCBROCMJDH

35. Asymmetric encryption is also known as?

a) Private key cryptography
b) Public key cryptography
c) Public private key cryptography
d) Traditional cryptography

36. Columnar cipher falls under the category of?

a) mono-alphabetic cipher
b) poly-alphabetic cipher
c) transposition cipher
d) additive cipher

37. How many columns do we need to have in the table, that is used for encryption in columnar transposition cipher when a given keyword is “SECRET” and plain text is “SANFOUNDRY”?

a) 4
b) 5
c) 6
d) 7

38. What will be the encrypted text corresponding to plain text “CLASSIFIED” using columnar transposition cipher with a keyword as “GAMES”?

a) LFDSIASECI
b) SECIAISDFL
c) CILFAISESD
d) LFSECIAISD

39. How many rows will the letters of the plain text occupy in the table, that is used for encryption in columnar transposition cipher when a given keyword is “SECRET” and plain text is “SANFOUNDRY”?

a) 1
b) 2
c) 3
d) 4

40. What will be the encrypted text corresponding to plain text “SANFOUNDRY” using keyed transposition cipher with a keyword as “GAMES” ?

a) SUANNDFROY
b) ANFRSUNDOY
c) NDSUFRANOY
d) SANFOUNDRY

41. If there is symmetric communication among 5 persons, how many of secret key is need ?

a) 5
b) 6
c) 10
d) 20

42. AES uses a _____ bit block size and a key size of _____ bits.

a) 128; 128 or 256
b) 64; 128 or 192
c) 256; 128, 192, or 256
d) 128; 128, 192, or 256

43. How many rounds does the AES-192 perform?

a) 10
b) 12
c) 14
d) 16

44. How many rounds does the AES-256 perform?

a) 10
b) 12
c) 14
d) 16

45. There is an addition of round key before the start of the AES round algorithms.

a) True
b) False