GOVERNMENT POLYTECHNIC, CHAPRA

Marhowrah, Saran, Bihar

COMPUTER NETWORK AND SECURITY
SUBJECT CODE – 2018602

6th SEM – Computer Science and Engineering

FACULTY NAME
Prof. Rama Singh
Contact No. – 8957601751

1. Which is not an objective of network security?
   a) Identification
   b) Authentication
   c) Access control
   d) Lock

2. The process of verifying the identity of a user.
   a) Authentication
   b) Identification
   c) Validation
   d) Verification

3. An algorithm in encryption is called _____
   a) Algorithm
   b) Procedure
   c) Cipher
   d) Module

4. The information that gets transformed in encryption is _____
   a) Plain text
   b) Parallel text
   c) Encrypted text
   d) Decrypted text

5. The _____ module in Pretty Good Privacy (PGP) uses MD5 to generate a hash code of the message and encrypts it with the sender's private key using an RSA algorithm.
   a) signature generation
   b) encryption
   c) email conversion
   d) compression

6. What do you mean by integrity protection in Security management?
   a) It makes sure that the information has not tampered as it traverses between the source and the destination
   b) It validates the originator identification
   c) It is used to overcome some of the problems identified in packet filtering
   d) It reduces the risk of access to hosts from an external network by filtering insecure services

7. In cryptography, the order of the letters in a message is rearranged by _____
   a) transpositional ciphers
   b) substitution ciphers
   c) both transpositional ciphers and substitution ciphers
   d) quadratic ciphers

8. 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

9. Cryptographic hash function takes an arbitrary block of data and returns _____
   a) fixed size bit string
   b) variable size bit string
   c) both fixed size bit string and variable size bit string
   d) variable sized byte string

10. Conventional cryptography also known as ... encryption.
    a) asymmetric-key
    b) logical-key
    c) symmetric-key
    d) None of these

11. Public key cryptography is a ... cryptosystem
    a) Symmetric
    b) Asymmetric
    c) Symmetric & Asymmetric both
    d) None of these

12. We are provided the plain text “SUN”. You need to convert the given plain text into ciphertext under the Ceasar cipher encryption technique. Which of the following options is the correct ciphertext for the given text if the key is 3?
    a) UWP
    b) VXQ
    c) WUP
    d) QSL

13. With symmetric key algorithms, the ____ key is used for the encryption and decryption of data.
    a) Different
    b) Same
    c) Both A and B
    d) None of the mentioned above

14. What is the full-form of RSA in the RSA encryption technique?
    a) Round Security Algorithm
    b) Rivest, Shamir, Adleman
    c) Robert, Shamir, Addie
    d) None of the above

15. Decryption is a process to unveil the _____.
    a) Unsecured data
    b) Secured data
    c) Insecure
    d) None of the mentioned above

16. Which of the following is /are offered by the Hash functions?
    a) Authentication
    b) Non repudiation
    c) Data Integrity
    d) All of the above

17. Which of the following is not possible through hash value?
    a) Password Check
    b) Data Integrity check
    c) Digital Signatures
    d) Data retrieval in its original form

18. Which of the following is an example of a hash function?
    a) SHA-1
    b) RSA
    c) AES
    d) Diffie-Hellman

19. Which of the following is a type of transposition cipher?

    a) Caesar cipher
    b) Playfair cipher
    c) Rail fence cipher
    d) Vigenere cipher

20. S/MIME is abbreviated as:
    a) Secure/Multimedia Internet Mailing Extensions
    b) Secure/Multipurpose Internet Mailing Extensions
    c) Secure/Multimedia Internet Mail Extensions
    d) Secure/Multipurpose Internet Mail Extensions

21. What are the possible results of an attack on a computer network? What are the best defenses against a brute force login attack?

22. Explain the difference between symmetric and asymmetric encryption.

23. Define the salting process and what it's used for. How do you deal with "Man in the Middle" attacks?

24. Which is the better security measure, HTTPS, or SSL? Name the three means of user authentication.

25. What are properties that a digital signature should have? Describe briefly playfair and Ceaser cipher.

26. What is RSA algorithm? Explain the process of public and private key generation and finally generating a ciphertext with an example.

27. What are various types of firewall? Explain each of them in detail.

28. Explain X.509 Certificate with diagram.

29. How does PGP create a secure network? Also explain PGP.

30. Compare and Contrast:

    a) Cryptography and Cryptanalysis
    b) Active and passive attack

31. What is Kerberos? Explain the Kerberos authentication system.

32. Compare and contrast Stream Cipher and Block cipher.

33. Write notes on:

    a) Non-repudiation

    b) VPN

    c) Digital certificate

34. Explain Secure electronic transaction and SNMP.

35. List out the components of encryption algorithm. Define integrity.

36. Convert the Given Text “CRYPTOGRAPHY” into cipher text using Rail fence Technique.

37. What are the different modes of operation in DES? What is purpose of S-boxes in DES?

38. What is the difference between differential and linear cryptanalysis? What are disadvantages of double DES?

39. What is Elliptic curve? What is the difference between Rijndael and AES?

40. What are the operations used in AES?

    a) Substitute bytes

    b) ShiftRows

    c) MixColumns

    d) AddRoundKey

41. Explain The RSA Algorithm And Explain RSA with P=7,Q=11,E=17,M=8. Discuss its merit.

42. What is the difference between public key and private key cryptosystem?

43. What is Message Authentication Code (MAC). How is it different from message digest?

44. Define hash function. Explain SHA-1 in detail. What do you mean by one way property in hash function?
45. Define digital signature. Explain the properties of Digital Signature. List out the attacks related to Digital Signature.
46. What is DSS? Mention the signature function in DSS.
47. How digital signature differs from authentication protocols?
48. Write down the steps involved in Elgamal DSS.
49. Define malicious software. What do you mean by trojan horse?
50. Write down the system security standards?
51. Define virus and worms. Specify the types of viruses?
52. State the difference between threats and attack? Define trusted system?
53. What do you mean by S/MIME? Explain its purpose. What are the types of MIME?
54. What are the function areas of IP security? Give the benefits of ip security?
55. Explain PKI and certificate authority.
56. What is the difference between TLS and SSL security?
57. What is operational model for network security? Explain with diagram.
58. What are side channel attacks? How can a side channel attack be done?
59. What do you mean by honeypot? Explain Mobile IP Security.
60. Explain RC4,RC5 and RC6 symmetric ciphers.