REV-01
MCA/44/49

2024/05

SET B

MASTER OF COMPUTER APPLICATION
FOURTH SEMESTER
CRYPTOGRAPHY & NETWORK SECURITY
MCA-401

[USE OMR SHEET FOR OBJECTIVE PART]

Duration: 3 hrs. **Full Marks: 70**

(Objective)

Time: 30 mins. **Marks: 20**

Choose the correct answer from the following: ***1×20=20***

1. In the DES algorithm the round key is .....bits and the Round Input is .....bits.
   a. 48, 32 b. 64, 32
   c. 56, 24 d. 32, 32
2. DES follows:
   a. Hash Algorithm b. Caesars Cipher
   c. Feistel Cipher Structure d. SP Networks
3. Which of these is a part of network identification?
   a. User id b. Password
   c. Otp d. Fingerprint
4. Public key encryption is advantageous over Symmetric key Cryptography because of:
   a. Speed b. Space
   c. Key exchange d. Key length
5. The security layer in WAP is between the.....layer and the..... layer.
   a. Transaction, transport b. Application, transport
   c. Transport, physical d. Session, transport
6. The two additional parameters to Password Based Encryption, other than the password are .....and.....
   a. Private key, public key b. Private key, salt
   c. Public key, salt d. Salt, iteration count
7. The .....protocol is similar to SSL.
   a. HTTP b. HTTPS
   c. TLS d. SHTTP
8. IP Sec provides security at the .....layer.
   a. Application b. Transport
   c. Network d. Data link
9. Kerberos provides for:
   a. Encryption b. SSO
   c. Remote login d. Local login
10. Password-based authentication is an example of .....authentication.
    a. 1-factor b. 2-factor
    c. 3-factor d. 4-factor

11. The DES Algorithm Cipher System consists of .....iterations each with a round key.
    a. 12 b. 18
    c. 9 d. 16

12. Biometric authentication works on the basis of:
    a. Human characteristics b. Passwords
    c. Smart cards d. Pin

13. The process of verifying the identity of a user is:
    a. Authentication b. Identification
    c. Validation d. Verification

14. The DES algorithm has a key length of:
    a. 128 bits b. 32 bits
    c. 64 bits d. 16 bits

15. Encryption Strength is based on:
    a. Strength of algorithm b. Secrecy of key
    c. Length of key d. All of the above

16. Which of the following is not a type of symmetric-key cryptography technique?
    a. Caesar cipher b. Data Encryption Standard
    c. Diffie Hellman cipher d. Playfair cipher

17. For RSA to work, the value of P must be less than the value of:
    a. p b. q
    c. n d. f

18. A process of making the encrypted text readable again is:
    a. Decryption b. Encryption
    c. Network security d. Information hiding

19. In public key cryptosystem .....keys are used for encryption and decryption.
    a. Same b. Different
    c. Encryption Keys d. None of the mentioned

20. Unsolicited Bulk E-mails (UBI) are called.....
    a. SMS b. MMS
    c. Spam emails d. Malicious emails

-- --- --

(Descriptive)

Time : 2 hr. 30 mins. Marks : 50

[Answer question no.1 & any four (4) from the rest]

1. What do you mean by cryptography? How many types of cryptographic techniques are there? Explain all of them with an example. 10
2. Differentiate between Data Encryption Standard Algorithm and Advance Encryption Standard Algorithm. 10
3. Explain the principles of the IDEA algorithm. 10
4. Explain Rivest-Shamir-Adleman algorithm in details along with an example. 10
5. Explain the different ways to use hashing for message authentication. 10
6. What do you mean by firewall? How many types of firewalls are there? Explain all of them with an example. 10
7. Explain the CIA model of network security in details along with examples. 10
8. What do you mean by SSL? Explain the various types of SSL protocols used in Transport Layer Security. 10

= = *** = =