Total No. of printed pages = 4

BCA 171502

Roll No. of candidate | | | | | | | | | | |

14/2/22 2021

B.C.A. 5th Semester End-Term Examination

NETWORK SECURITY AND CRYPTOGRAPHY

(New Regulation)

Full Marks – 70 Time – Three hours

The figures in the margin indicate full marks for the questions.

Answer question No. 1 and any *four* from the rest.

1. Answer the following questions : (10 × 1 = 10)

(i) 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

(ii) 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

(iii) Which of the following is not a principle of data security?

(a) Data Confidentiality

(b) Data Integrity

(c) Authentication

(d) None of the above

[Turn over

(iv) Which of the following security attacks is not an active attack?

- (a) Masquerade
- (b) Modification of message
- (c) Denial of service
- (d) Traffic analysis

(v) "A key is a string of bits used by a cryptographic algorithm to transform plain text into cipher text." Which of the following is capable of becoming a key in a cryptographic algorithm?

- (a) An integer values
- (b) A square matrix
- (c) An array of characters (i.e. a String)
- (d) All of the above

(vi) A mechanism used to encrypt and decrypt data

- (a) Cryptography
- (b) Algorithm
- (c) Data flow
- (d) None of these

(vii) Conventional cryptography also known as ―――――― encryption.

- (a) asymmetric-key
- (b) logical-key
- (c) symmetric-key
- (d) None of these

(viii) Security Goals of Cryptography are

- (a) Confidentiality
- (b) Authenticity
- (c) Data integrity
- (d) Non-repudiation
- (e) All of these

(ix) Which of the following cipher techniques include the involvement of matrix operations in their algorithms of encryption and decryption?

- (a) Hill Cipher
- (b) Playfair cipher
- (c) Both (a) and (b)
- (d) None of the above

(x) 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

2. Answer the following questions

(a) What is passive device in terms of network security? Explain how it is different from active devices? (5)

(b) Explain the security threat Masquerading with suitable example. (5)

(c) Explain the relation between the different security services and security mechanism. (5)

3. Answer the following questions

(a) Explain the encryption and Decryption process of Hill Cipher considering plaintext "INDIA" and key" (7)

$$\begin{bmatrix} 2 & 3 \\ 3 & 6 \end{bmatrix}$$

(b) Explain Vernam Cipher Encryption and Decryption process considering plaintext as "JORHAT" and Key as "ACTIVE" (2 × 4 = 8)

4. Answer the following questions

(a) What is Symmetric Encryption? What are the different types of Symmetric Encryption technique? Explain with example. (7)

(b) Explain with suitable example the difference between Monoalphabetic Cipher and Polyalphbetic Cipher? (5)

(c) Explain the working procedure of PlayFair Cipher. (3)

5. Answer the following questions

(a) Caesar Cipher is Monoalphabetic or Polyalphbetic cipher? Considering the plaintext as "HIMALAYA" and Key=5. Explain the Encryption and Decryption Technique using Caesar Cipher Encryption Technique. (2+3+3=8)

(b) What is a Digital Signature? Explain the working of Digital Signature. (7)

6. Answer the following questions

(a) Explain security threat Replaying with an example. (3)

(b) Considering the plaintext as "CRICKET" and Key is "BALL". Explain the Encryption and Decryption Technique using PlayFair Symmetric Encryption Technique. (2 × 4 = 8)

(c) Explain how Vigenere Cipher Technique works considering Plaintext "TELEPHONE" and key "MOBILE". (4)

7. Answer the following questions

(a) Explain the goals of network security. (4)

(b) What is Repudiation? Explain with example. (5)

(c) What is the difference between Snooping and Spoofing. (6)