

Roll No.

Total No. of Pages : 02

Total No. of Questions : 09

B.Tech. CSE (Internet of Things and Cyber Security including Block Chain Technology) (Sem.-6)

NETWORK SECURITY & CRYPTOGRAPHY

Subject Code : BTCS701-18

M.Code : 93411

Date of Examination : 17-05-2023

Time : 3 Hrs.

Max. Marks : 60

INSTRUCTIONS TO CANDIDATES :

1. **SECTION-A is COMPULSORY** consisting of **TEN** questions carrying **TWO** marks each.
2. **SECTION-B** contains **FIVE** questions carrying **FIVE** marks each and students have to attempt any **FOUR** questions.
3. **SECTION-C** contains **THREE** questions carrying **TEN** marks each and students have to attempt any **TWO** questions.

SECTION-A

1. Write briefly :

- a. Define protocol vulnerability.
- b. Define cryptanalysis.
- c. What is Euclidean distance?
- d. What are properties of prime numbers for the safety of encrypted messages?
- e. Structure of Feistel cipher.
- f. List few principles of public key cryptography.
- g. What are digital signatures?
- h. List few key distribution techniques.
- i. Why do we need honeypots?
- j. List few tools used for traffic monitoring.

SECTION-B

2. Explain the conventional encryption model. Discuss few important requirements for secure use of conventional encryption.
3. Explain the Euclidean algorithm used for finding GCD of two numbers for cryptography.
4. Explain the Diffie Hellman key exchange algorithm for key management in cryptography.
5. What are hash functions? Discuss about secure hash functions.
6. What is a firewall? Discuss the differences between IPS firewall and IDS.

SECTION-C

7. What are active and passive threats? Discuss different vulnerabilities present in the protocols, Internet architecture that helps the attackers to launch active and passive threats.
8. What are block cipher? Explain the DES algorithm for block cipher. Why there is need to extend DES to double and triple DES?
9. Write a short note on :
 - a. CIA Model
 - b. S/MIME vs. PGP

NOTE : Disclosure of Identity by writing Mobile No. or Making of passing request on any page of Answer Sheet will lead to UMC against the Student.