CBCS SCHEME

USN | | | | | | | | | | |

15CS61

Sixth Semester B.E. Degree Examination, June/July 2023
Cryptography, Network Security and Cyber Law

Time: 3 hrs. Max. Marks: 80

Note: ***Answer any FIVE full questions, choosing ONE full question from each module.***

Module-1

1 a. List and explain the various types of vulnerabilities with common cyber attacks. **(08 Marks)**

b. Encrypt the plaintext "CRYPTOGRAPHY" using hill cipher technique with key matrix $K = \begin{bmatrix} 9 & 4 \\ 5 & 7 \end{bmatrix}$. **(08 Marks)**

OR

2 a. Distinguish between :
i) Confusion and diffusion ciphers ii) Block cipher and stream ciphers. **(08 Marks)**

b. With a neat schematic, explain the single round of DES encryption model. **(08 Marks)**

Module-2

3 a. Explain RSA operation in detail. **(05 Marks)**

b. Explain Public Key Cryptography Standards (PKCS). **(05 Marks)**

c. Explain Deffie Helman key exchange. **(06 Marks)**

OR

4 a. If the RSA public key is (31, 3599) what is the Corresponding Private Key. **(05 Marks)**

b. Explain Basic properties of hash function. **(05 Marks)**

c. Explain Birthday attack. **(06 Marks)**

Module-3

5 a. Explain the different Public Key Infrastructure (PKI) architectures. **(08 Marks)**

b. Describe the Mutual authentication using a shared secret. **(08 Marks)**

OR

6 a. Explain the Kerberos message sequence with diagram. **(06 Marks)**

b. Describe the IP Sec protocols Authentication Header and Encapsulating Security Pay load in transport mode. **(05 Marks)**

c. Explain Secure Sockets Layer (SSL) hand shake protocol. **(05 Marks)**

Module-4

7 a. What is intrusion detection system (IDS)? Explain different types of IDS. **(06 Marks)**

b. Explain how 802.11i provides message confidentiality and integrity. **(06 Marks)**

c. Explain the characteristics of virus and worm. **(04 Marks)**

OR

8 a. What is WS-security? Explain the various types of WS – security. **(06 Marks)**

b. Explain the prevention and detection methods on DDOS attack. **(06 Marks)**

c. List and explain any two technologies used for web services. **(04 Marks)**

Module-5

9 a. Discuss OFFENES defined as per IC Act 2000 (any four). **(08 Marks)**

b. Explain briefly Certifying authority , Suspensions and Revocations of digital signature. **(08 Marks)**

OR

10 a. What is Information Technology Act? Discuss scope and objectives. **(08 Marks)**

b. Discuss the provisions of the IT Act as regards to the following :

i) Legal Recognition of Electronic records   ii) Authentication of Electronic records. **(08 Marks)**

* * * * *