CBCS SCHEME

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

15CS61

Sixth Semester B.E. Degree Examination, June/July 2024
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. What are the common cyber attacks? Explain different defense strategies to prevent cyber attacks. **(06 Marks)**

b. Write extended Euclidean algorithm. And find 77^{-1} Mod 411 using extended Euclidean algorithm. **(08 Marks)**

c. Distinguish between confusion and diffusion. **(02 Marks)**

OR

2 a. Explain the construction of DES with Fiestal structure. **(05 Marks)**

b. Encrypt the plaintext "CRYPTOGRAPHY" using Hill cipher with key $K = \begin{bmatrix} 7 & 8 \\ 19 & 3 \end{bmatrix}$ **(06 Marks)**

c. Prove that $<Z_7, +_7, *_7>$ is a field. **(05 Marks)**

Module-2

3 a. Illustrate the RSA algorithm for encryption and decryption. **(08 Marks)**

b. Briefly explain the practical issues of RSA algorithm. **(04 Marks)**

c. List the properties of the cryptographic hash. **(04 Marks)**

OR

4 a. Discuss the case study : SHA – I. **(08 Marks)**

b. Explain the Man – In – the Middle attack on Diffie – Hellman key exchange, with neat diagram. **(08 Marks)**

Module-3

5 a. What do you mean key management? Explain the fields of an X.509 certificate. **(06 Marks)**

b. List and explain PKI Architectures. **(06 Marks)**

c. Define Dictionary Attacks. Explain Attack types. **(04 Marks)**

OR

6 a. Design the Needham – Schroeder protocol. **(06 Marks)**

b. Define Kerberos. Explain Kerberos message sequence. **(05 Marks)**

c. Explain SSL Record Layer Protocol. **(05 Marks)**

Module-4

7 a. What are the tasks performed by intrusion detection system? Briefly explain the different types of intrusion detection system. **(08 Marks)**

b. Explain 4 way handshake in 802.11i. **(08 Marks)**

OR

8 a. What is a firewall? Explain the functions of firewall. **(08 Marks)**

b. Briefly explain the different technologies used for web services. **(08 Marks)**

Module-5

9 a. Explain Digital Signature Certificates. **(10 Marks)**

b. Describe the duties of Subscribers. **(06 Marks)**

OR

10 a. List any eight functions of the Controller. **(08 Marks)**

b. Briefly explain Penalties and Adjudicaiton in IT Act. **(08 Marks)**

* * * * *