



# CBCS SCHEME

--	--	--	--	--	--	--	--	--	--

17CS61

## Sixth Semester B.E. Degree Examination, Jan./Feb. 2023 Cryptography, Network Security and Cyber Law

Time: 3 hrs.

Max. Marks: 100

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

### Module-1

- 1 a. Explain common attacks and vulnerabilities in cyber attacks with a diagram. (10 Marks)
- b. Write the Extended Euclidean algorithm and compute the inverse of 12 module 79. (10 Marks)

OR

- 2 a. Calculate the value of  $x$  using Chinese remainder theorem by given data  $N = 210$ ,  $n_1 = 5$ ,  $n_2 = 6$ ,  $n_3 = 7$ ,  $x_1 = 3$ ,  $x_2 = 5$ ,  $x_3 = 2$ . (10 Marks)
- b. Consider a hill cipher  $m = 2$  [Block size = 2] with plain text (H, I) and key  $k$  is  $k = \begin{pmatrix} 3 & 7 \\ 15 & 12 \end{pmatrix}$ . Obtain the cipher text. (10 Marks)

### Module-2

- 3 a. Illustrate the RSA algorithm for encryption and decryption for the given data  $p = 3$ ,  $q = 11$ ,  $e = 3$  and  $m = 20$ . (10 Marks)
- b. With a neat diagram explain the construction of SHA-1. (10 Marks)

OR

- 4 a. With regard to cryptographic hash, explain the Hash-based MAC and digital signature. (10 Marks)
- b. Explain Diffie – Hellman key exchange with an example. (10 Marks)

### Module-3

- 5 a. List and explain PKI architectures with a neat diagram. (08 Marks)
- b. Define Key Management? Explain the fields of X.509 certificate. (06 Marks)
- c. Describe Mutual authentication using a shared secret. (06 Marks)

OR

- 6 a. Explain Needham – Schroeder protocol Version-2. (06 Marks)
- b. Explain the Kerberos with message sequence. (06 Marks)
- c. Explain SSL handshake protocol. (08 Marks)

### Module-4

- 7 a. Explain authentication and master session key exchange in 802.11i. (08 Marks)
- b. List and explain worm characteristics. (06 Marks)
- c. Explain firewall functionality and proxy firewall. (06 Marks)

OR

- 8 a. Explain the types of intrusion detection system. (08 Marks)
- b. What is SOAP? Explain SOAP messages in HTTP packets. (06 Marks)
- c. With regard to web services security, discuss the XML signatures. (06 Marks)

**Module-5**

- 9 a. Discuss OFFENCES defined as per IT Act 2000 [Any five]. (10 Marks)  
b. List and explain important provisions as per IT Act 2000[Any five]. (10 Marks)

**OR**

- 10 a. Explain Secure Electronic Record and Secure Digital Signatures in IT Act 2000. (06 Marks)  
b. List and explain functions of controller in IT Act 2000. (06 Marks)  
c. List and explain cyber regulations appellate Tribunal in IT Act 2000 [Any four]. (08 Marks)

\* \* \* \* \*