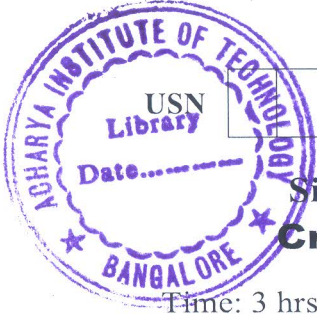


# CBCS SCHEME



15CS61

## Sixth Semester B.E. Degree Examination, July/August 2021 Cryptography, Network Security and Cyber Law

Time: 3 hrs.

Max. Marks: 80

Note: Answer any FIVE full questions.

- 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  $77^{-1} \text{ Mod } 411$  using extended Euclidean algorithm. (08 Marks)
- c. Distinguish between confusion and diffusion. (02 Marks)
- 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  $\langle \mathbb{Z}_7, +_7, *_7 \rangle$  is a field. (05 Marks)
- 3 a. Describe RSA algorithm. Perform encryption and decryption using the RSA algorithm for  $p = 3, q = 11, e = 17$  and  $m = 8$ . (08 Marks)
- b. What is a hash function? Explain the properties of hash function. (04 Marks)
- c. Explain the computation of Hash based MAC (HMAC). (04 Marks)
- 4 a. Describe the computation of SHA-1 algorithm. (08 Marks)
- b. Explain Diffie hellman key exchange protocol with an example. (08 Marks)
- 5 a. What is digital certificate? Explain general format of X.509 certificate. (06 Marks)
- b. Explain Needham Schroeder protocol preliminary version 1. (10 Marks)
- 6 a. Describe the IP security protocols in transport mode. (08 Marks)
- b. Explain SSL handshake protocol. (08 Marks)
- 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)
- 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)
- 9 a. What is Information Technology Act? Discuss its aims and objectives and scope. (08 Marks)
- b. Who is a controller? Outline his functions and powers. (08 Marks)
- 10 a. Describe the duties of subscribers. (08 Marks)
- b. Describe the following terms under the Information Technology Act, 2000:  
i) Addressee      ii) Certifying Authority      iii) Secure system      iv) Digital signature  
v) Electronic record      vi) Intermediary      vii) Cyber applet tribunal      viii) Information. (08 Marks)

Important Note : 1. On completing your answers, compulsorily draw diagonal cross lines on the remaining blank pages.  
2. Any revealing of identification, appeal to evaluator and /or equations written eg.  $42+8=50$ , will be treated as malpractice.

\* \* \* \* \*