

CBCS SCHEME



USN

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

15CS61

Sixth Semester B.E. Degree Examination, June/July 2019 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. Describe the types of Vulnerabilities to domain of security. (04 Marks)
- b. List the guiding principles of security. (04 Marks)
- c. Write the extended Euclidean algorithm, with an example. (08 Marks)

OR

- 2 a. Calculate the value of x using Chinese remainder theorem by given below data :
 $N = 210$, $n_1 = 5$, $n_2 = 6$, $n_3 = 7$, $x_1 = 3$, $x_2 = 5$, $x_3 = 2$. (05 Marks)
- b. Explain the Vigenere Cipher and the Hill Cipher techniques with illustration. (06 Marks)
- c. With neat diagram, explain Fiestel structure. (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. 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. Explain the Authentication and Master Session Key exchange in 802.11i. (05 Marks)
- b. List and explain the worm characteristics. (05 Marks)
- c. Explain Firewall functionality and Proxy fire wall. (06 Marks)

OR

- 8 a. Write a note on Intrusion Detection System (IDS). (05 Marks)
- b. Explain the types of Intrusion Detection System. (05 Marks)
- c. Briefly explain the Technologies for Web Services. (06 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 Adjudication in IT Act. (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.