

USN

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

15CS61

Sixth Semester B.E. Degree Examination, Dec.2018/Jan.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. Define cyber security? Explain the motives of cyber attack. (05 Marks)
- b. Use extended Euclidean algorithm to find inverse of 12 modulo 79? (05 Marks)
- c. Apply Chinese reminder theorem to find square roots of 3 modulo 143 and list all square roots of -3 modulo 143. (06 Marks)

OR

- 2 a. Explain DES construction in detail. (05 Marks)
- b. Explain confusion and Diffusion with example. (05 Marks)
- Explain three sounds SPN Network. (06 Marks)

Module-2

- 3 a. Explain RSA operation in detail. (06 Marks)
- b. Explain Public Key Cryptography Standards (PKCS) (10 Marks)
- c. Explain Deffie Helman key exchange.

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 identity based encryption. (05 Marks)
- b. Explain Needham Schroeder protocol version – 1. (05 Marks)
- c. Explain Kerberos with message sequence. (06 Marks)

OR

- 6 a. Explain password based one way authentication. (05 Marks)
- b. Explain Needham – Schroeder protocol version – 2. (05 Marks)
- c. Explain SSL Handshake protocol. (06 Marks)

Module-4

- 7 a. Explain authentication and master session key exchange in 802.11i? (05 Marks)
- b. Explain worm features. (05 Marks)
- c. Explain Function of Firewall. (06 Marks)

OR

- 8 a. Explain 802.11i four way handshanke with neat diagram. (05 Marks)
- b. List and explain practice issues of Firewall. (05 Marks)
- c. Explain DDOS attack prevention and detection. (06 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)

* * * * *