

USN

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

15CS61

## Sixth Semester B.E. Degree Examination, July/August 2022 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. Explain common attacks with respect to cyber space. (06 Marks)
- b. Apply extended Euclidean algorithm to find the inverse of 12 modulo 79. (04 Marks)
- c. Distinguish between the following:
  - (i) Stream and Block Cipher. (06 Marks)
  - (ii) Substitution and Transposition cipher (06 Marks)

**OR**

- 2 a. Explain different classes of vulnerabilities in the domain of network security. (06 Marks)
- b. Describe the various kinds of cryptanalysis attack. (04 Marks)
- c. With a neat diagram demonstrate the working of DES algorithm. (06 Marks)

### Module-2

- 3 a. The modulus (n) in a toy implementation of RSA is 143 and the encryption key (e) is 11. Find the corresponding decryption key and encrypt plain text = 127. (08 Marks)
- b. What is the common secret key if A and B perform Diffie-Hellman key exchange using  $P = 53$  and  $g = 2$ . Assume the secret key of A is 10 and B is 33. (04 Marks)
- c. Block of plain text has been encrypted using Elgamal encryption with  $P = 131$ ,  $g = 2$  and the recipient's public key ( $\alpha$ ) = 14. What is the plain text corresponding cipher text  $C_1 = 103$  and  $C_2 = 51$  [Sender's private key  $a = 97$ ]. (04 Marks)

**OR**

- 4 a. Explicate the properties of hash algorithm. (04 Marks)
- b. Elaborate on the practical issues of RSA. (08 Marks)
- c. Narrate man-in-the middle attack on Diffie Hellman key exchange. (04 Marks)

### Module-3

- 5 a. With a neat diagram, explain function of SSL record layer protocol. (08 Marks)
- b. Illustrate the various steps in Kerberos message sequence. (08 Marks)

**OR**

- 6 a. Explain AH and ESP in tunnel mode of IP security. (08 Marks)
- b. Describe mutual authentication using shared secret. Also identify the solution to overcome the issues posed by it. (08 Marks)

### Module-4

- 7 a. Define web services as defined by  $\omega^3C$ . Discuss the entities involved in web services. (06 Marks)
- b. Explain the functions of WS-security. (10 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.

**OR**

- 8 a. Differentiate Anomaly V/s Signature based IDS. (04 Marks)  
b. Discuss the characteristics of worms. (06 Marks)  
c. Depict four-way handshake in 802.11i. (06 Marks)

**Module-5**

- 9 a. Define the following terms under the IT Act 2000:  
(i) Addressee  
(ii) Subscriber  
(iii) Adjudicating officer.  
(iv) Originator.  
(v) Certifying authority. (05 Marks)  
b. What is Information Act? Discuss its aim, objective and scope of the act. (07 Marks)  
c. Outline any four functions of controller. (04 Marks)

**OR**

- 10 a. Discuss the provisions of IT Act with respect to Authentication of electronic record. (06 Marks)  
b. Explain the duties of subscriber. (06 Marks)  
c. Define the penalty for failure to furnish information return under section 43 of IT Act 2000. (04 Marks)

\* \* \* \* \*