USN | 1 | S | I | | | | | | | |

MOBILE PHONES PROHIBITED

1RSCS02/1RSCN02

Siddaganga Institute of Technology, Tumakuru – 572 103

(An Autonomous Institution affiliated to VTU, Belagavi, Approved by AICTE, New Delhi)

First Semester M.Tech. Examinations Feb. 2020

Cryptography & Network Security

Common to SCS/SCN

Time: 3 Hours **Max. Marks: 100**

Note : Answer any five questions choosing one full question from each unit.

Unit - I

1 a) State the purpose of Extended Euclid algorithm. Apply the algorithm on 1629 and 384 to obtain the desired outputs. 07

b) Verify whether the following are groups. If yes, find the inverse of each element.
i. Z5 under addition ii. Z7 under multiplication 06

c) What is cyclic group? Show that fourth roots of unity namely {1, -1, i, -i} is a cyclic group. 07

OR

2 a) Classify the cryptography using various criteria. What do you understand by “computationally secure” and “unconditionally secure” algorithms? 06

b) Compute the ciphertext for the message “WONDERFUL” using the Hill cipher technique. Given key is “SUNDAY”. 08

c) Encrypt the message “PINEAPPLE” using Playfair cipher. Given key is “PRAYER”. 06

Unit - II

3 a) Elaborate the terms P-box and S-box with respect to symmetric ciphers by explaining various types. 08

b) Explain the classical Fiestal cipher structure. Identify the choice of various parameters that impart security to encryption algorithms. 08

c) Differentiate between confusion and diffusion. 04

OR

4 a) Mention the types of cryptanalysis attacks on block ciphers and describe each with suitable terms. 10

b) With necessary block diagrams and pseudo-codes, outline the processing steps involved in the AES algorithm. 10

Unit - III

5 a) How confidentiality and authentication can be achieved together using public key cryptosystem? Elaborate with suitable notations. 04

b) Mention the steps involved in the RSA algorithm. Given p=7, q=19 and e=5, show the encryption and decryption of M=32. 08

c) Find the solution to the system of modular equations given below.

$$a \equiv 4 \pmod{7}$$
$$a \equiv 3 \pmod{8}$$
$$a \equiv 5 \pmod{9}$$

08

OR

6 a) State the significance of Euler’s phi function. Find the value of $\phi(54)$. 04

b) With suitable terms and sequence diagrams, describe the challenge response authentication using symmetric and asymmetric key ciphers. 08

c) Mention the design objective of HMAC. With a suitable HMAC structure diagram, explain the overall operation of HMAC. 08

Unit – IV

7 a) Mention the strategies to secure traffic generated by the websites at different layers. 06

b) Draw the SSL protocol graph. Describe the SSL Alert protocol. 06

c) With a timing diagram explain the handshaking protocol used in SSL. Give details of each phase. 08

OR

8 a) Discuss the operation of PGP protocol. With the help of message format diagram, identify the importance of each field in the operation. 10

b) Elaborate the operation of various key rings in the PGP and state the level of security. 10

Unit – V

9 a) Highlight the various applications of IPSec. 06

b) Interpret the term “Security Association” in IPSec. Mention the various parameters involved. 06

c) With an ESP packet format diagram, state the importance of each field. Discuss the padding process involved. 08

OR

10 a) Identify the approaches to intrusion detection. Discuss their working principles, pros and cons. 08

b) Write a short note on backdoor w.r.t. Malicious software. 06

c) Identify the various phases of computer virus operation. 06