



I SEMESTER M. TECH (COMPUTER NETWORKING AND ENGINEERING)

END SEMESTER EXAMINATIONS, NOVEMBER 2018

SUBJECT: INFORMATION SECURITY [ICT 5103]

REVISED CREDIT SYSTEM

(24/11/2018)

Time: 3 Hours

MAX. MARKS: 50

Instructions to Candidates:

- ❖ Answer ALL the questions
- ❖ Missing data may be suitably assumed.

- 1A. Describe paging and segmentation memory protection techniques used in general purpose operating systems. Give the necessary data structures to carryout memory mapping. Does the combination of these two techniques give better performance in terms of memory protection and usage? Explain with suitable diagrams. (05)
- 1B. Let \circ be the composition operation on the two permutations formed from the set $\{1,2,3\}$. Prepare the operation table defining \circ for permutation group. (03)
- 1C. With a neat diagram explain the database recovery technique in cloud. (02)
- 2A. How can you ensure the application-level authentication using Kerberos V4 protocol in multiple realms? Explain in detail with suitable diagram and authentication dialogs. (05)
- 2B. Find the cyclic subgroups that can be created from the group $G = \langle \mathbb{Z}_8, + \rangle$. (03)
- 2C. Differentiate between cryptographic and biometric authentication techniques. (02)
- 3A. Determine the multiplicative inverse of (x^4+x^3+1) in $GF(2^5)$ with modulus (x^5+x^2+x+1) . (05)
- 3B. What are the different design of multilevel secure databases? Explain with neat diagrams. (03)
- 3C. Differentiate between hierarchical PKI and mesh PKI with neat diagrams. (02)
- 4A. Explain two layered architecture of SSL security protocol. What is the difference between SSL session and SSL connection? Explain different parameters to be exchanged between the partners during communication. (05)
- 4B. With a neat diagram explain x509.v3 digital certificate. Mention any two applications that use this certificate for user authentication. (03)
- 4C. Describe briefly the legal, privacy and ethical issues in computer security. (02)

- 5A.** With neat diagrams explain different firewall configuration techniques. (05)
- 5B.** Explain the following security problems associated with cloud computing.
- i. Loss of control
 - ii. Lack of trust
 - iii. Multitenancy
- (03)
- 5C.** Mention the technology used for linking the two messages intended for merchant and bank. How does it link these messages? (02)