Paper / Subject Code: 89379 / System Security (DLOC - VI)

(3 Hours) **Total Marks: 80**

Note:
1. **Question No. 1 is compulsory**.
2. Attempt any **THREE** out of the remaining **FIVE** questions.
3. Assume suitable data if necessary.

Q. 1 **20 marks**

A What are the primary security goals. The following attacks are a threat to which security goals: 5 marks
Snooping, traffic analysis, modification, masquerading, replay, repudiation, traffic analysis.

B How to collect audit data for security auditing and analysis. 5 marks

C Differentiate between symmetric and asymmetric ciphers 5 marks

D Discuss the format of X. 509 certificate 5 marks

Q. 2 **20 marks**

A Explain the concept of asymmetric key cryptography with respect to knapsack cryptosystem. 10 marks
Given the super increasing tuple b= (2, 3, 7, 15, 31), r=41 and modulus n=61. Encrypt M=01101 using knapsack cryptosystem. Show the process of decryption as well.

B Differentiate between AES and DES 10 marks

Q. 3 **20 marks**

A Two users wish to establish a secure communication channel and exchange a session key after mutual authentication. Show how this can be done with the help of a Kerberos. 10 marks

B Why is a firewall considered a crucial component of network security infrastructure? How do different firewalls differ in their approach to filtering network traffic? 10 marks

Q.4 **20 marks**

A Explain the following Web Browser Attacks: 10 marks
Account Harvesting, Web Bugs, Clickjacking, CrossSite Request Forgery, Session Hijacking

B How is security achieved in Transport and Tunnel modes of IPSEC? Explain role of AH and ESP 10 marks

Q.5 **20 marks**

A Describe IoT attacks and its countermeasures. 10 marks

B Briefly explain Mobile Security. 10 marks

Q.6 **20 marks**

A A user wishes to do online transactions with Flipkart.com. Discuss a protocol which can be used to set up a secure communication channel and provide server side and client-side authentication. Show the steps involved in the handshake process. 10 marks

B Describe cloud identity and access management. 10 marks
