

Roll No. ....

Printed Pages : 2

**8707**

**BT-7/D12**

**SECURITY AND CRYPTOGRAPHY**

**Paper-CSE-473**

*Time allowed : 3 hours]*

*[Maximum marks : 75*

*Note : Attempt five questions by selecting at least one question from each unit.*

**Unit-I**

1. What do you understand by crypto-analysis ? Discuss various types of ciphers and principles of cryptography. 15
2. Describe the strengths and weaknesses of following crypto algorithms :
  - (a) DES
  - (b) RSA
  - (c) IDEA.

**Unit-II**

3. Discuss following terms/concepts : 15
  - (a) shared-secret key
  - (b) kerberos
  - (c) digital signatureGive examples for illustration.

**8707**

[Turn over

( 2 )

4. Describe following algorithms : 15
  - (a) KDC family of protocols.
  - (b) Needham-Schroeder Protocol
  - (c) Secure Hash algorithm.

**Unit-III**

5. What do you mean by computer security ? Describe various threats to and mechanisms for computer security. 15
6. Describe different types and flavours of "malicious code". Discuss the mechanism of their working and the way they are dealt with. 15

**Unit-IV**

7. Answer following parts : 15
  - (a) Threats to network security and preventing the loss/damage.
  - (b) Network security plan and policy.
  - (c) Virtual Private Networks.
8. Discuss following topics in network security context : 15
  - (a) Firewalls and its types.
  - (b) Security of network components
  - (c) Controlling the access at various levels.

**8707**