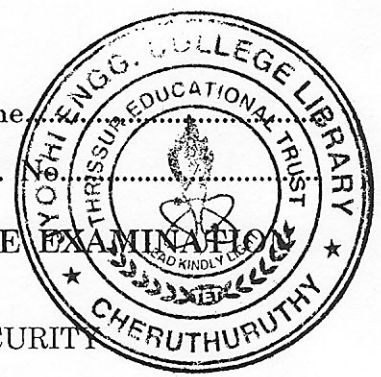


C 5511

Name

Reg.



SEVENTH SEMESTER B.TECH. (ENGINEERING) DEGREE EXAMINATION  
JUNE 2010

CS/IT 04 702-CRYPTOGRAPHY AND NETWORK SECURITY

(2004 admissions)

Time : Three Hours

Maximum : 100 Marks

- I. 1 State and prove the Fermat's theorem.  
2 Discuss the different types of security services.  
3 Explain any two methods of random number generation.  
4 What are all the possible attacks while communication takes place across a network ?  
5 Explain the achievements of security in DSA.  
6 How the encrypted data are computed while broadcasting ?  
7 Draw the general format of PGP message.  
8 Explain the different intrusion techniques briefly.
- (8 × 5 = 40 marks)
- II. (a) (i) State and encrypt the word MESSAGE WILL BE GIVEN LATER using transposition technique. (8 marks)
- (ii) Discuss about steganography. (7 marks)
- Or*
- (b) (i) Write notes on differential cryptanalysis. (10 marks)
- (ii) What are special characteristics of Blowfish ? (5 marks)
- III. (a) Explain the significance of two party Diffie-Hellman key exchange protocol and also discuss how will you expand this multiparty system. (15 marks)
- Or*
- (b) Describe MAC. Explain the requirements of MAC. (15 marks)
- IV. (a) Explain briefly about Feige-Fiat Shamir scheme. (15 marks)
- Or*
- (b) Describe the Fair and Fail safe cryptosystems. (15 marks)
- V. (a) Explain in detail about Kerberos with example. (15 marks)
- Or*
- (b) What are the services offered by IPSEC ? Explain in detail. (15 marks)

[4 × 15 = 60 marks]