(MODEL QUESTION PAPER)

Sixth Semester B.Tech Degree Examination (2013 Scheme)

Branch: Information Technology

13.602: Cryptography (F)

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

PART A

(Answer all questions. Each carries 4 marks)

1. Explain in detail about substitution ciphers.
2. What are the draw backs of double DES and why do we go for triple DES?
3. How is a knapsack system cracked?
4. What is a Fair cryptosystem?
5. Explain message authentication with MAC.

PART B

(Answer any one full question from each module)

Module I

6. a) Explain in detail the various aspects of security. (8)
   b) Explain in detail the working of a Hagelin machine. (7)
   c) Eve has intercepted the ciphertext "UVACLYFZLJBYL". Show how she can use an exhaustive key search to break this Caesar cipher. (5)

OR

7. a) What are the different types of cryptanalytic attacks? (8)
   b) The encryption key in a transposition cipher is (3,1,4,5,2). Perform encryption and decryption for the message "meet me after the toga party". Add a bogus character at the end to make the last group the same size as the others. (5)
   c) What is the role of Coincidence index in cryptanalysis? Prove that CI' is a pure estimator of CI. (7)

Module II

8. a) Explain the algorithm of DES in detail with necessary diagrams. (12)
   b) Explain Golomb's criteria for pseudorandom sequences. (4)
   c) What are weak keys and semi-weak keys of DES? (4)

OR

9. a) Explain the structure and working of IDEA. (8)

b) What are the different modes of DES? Explain any two. (8)

c) Explain how LSFRs are analyzed based on generating functions. (4)

Module III

10. a) Explain RSA system. Prove that the RSA decryption indeed recovers the original plaintext. (12)

b) Explain in detail about the Diffie-Hellman protocol for key distribution in asymmetrical systems. (8)

OR

11. a) Discuss public key systems based on elliptic curves. (12)

b) Explain the different encipherment methods implemented in a network for data security. (8)

Module IV

12. a) What is a Birthday attack? Explain. (4)

b) Briefly explain the Digital Signature Algorithm (DSA). (10)

c) Explain Zero knowledge techniques. (6)

OR

13. a) Explain in detail about the two-way challenge-response and three-way challenge-response for entity authentication with symmetrical algorithm. (10)

b) Define Kerberos and name its servers. Briefly explain the duties of each server. (10)