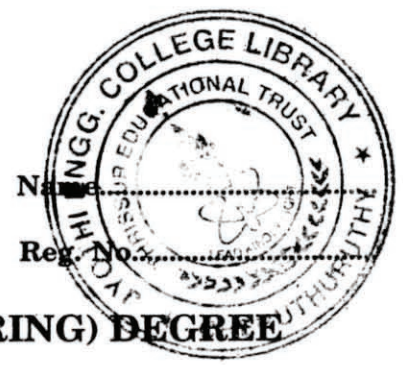


C 44405



**SEVENTH SEMESTER B.TECH. (ENGINEERING) DEGREE  
EXAMINATION, JUNE 2013**

CS/IT/PTCS 09 704 – CRYPTOGRAPHY AND NETWORK SECURITY

(2009 Scheme – Supplementary)

Time : Three Hours

Maximum : 70 Marks

**Part A**

- I. (a) What is cryptanalysis and cryptography?  
(b) Define threat and attack.  
(c) Mention any *two* techniques of attacking RSA.  
(d) What do you mean by hash function?  
(e) Define S/MIME.

(5 × 2 = 10 marks)

**Part B**

- II. (a) Compare Substitution and Transposition techniques.  
(b) What is meant by triple encryption?  
(c) List important design considerations for a stream cipher.  
(d) What is a meet-in-the-middle attack?  
(e) What are the header fields defined in MIME?  
(f) What are the security options PGP allows when sending an email message?

(4 × 5 = 20 marks)

**Part C**

- III. (a) Explain the DES Cipher with neat sketches.  
*Or*  
(b) Analyze the Feistel cipher structure and explain the Feistel encryption and decryption.
- IV. (a) Describe the RSA algorithm with an example and discuss its security.  
*Or*  
(b) Discuss Diffie Hellman Key Exchange algorithm.
- V. (a) Explain in detail Kerberos Version 5 authentication dialogues.  
*Or*  
(b) Give an overview on S/MIME functionality.
- VI. (a) Discuss in detail about Secure Electronic Transaction.  
*Or*  
(b) What are the characteristics of a Firewall? Explain the different types of Firewall with neat diagrams.

(4 × 10 = 40 marks)