(Following Paper ID and Roll No. to be filled in your Answer Books)

PAPER ID : ME23

Roll No.										

M. TECH. (Sem.II)

THEORY EXAMINATION 2015-16

CRYPTOGRAPHY

Time : 3 Hours Total Marks : 100

Note : Attempt all questions.

1. Answer any four of the following : (5×4=20)

(a) Explain finite field of the form GF(p).

(b) What is triple DES? Explain the term meet-in-the-middle attack.

(c) Explain the concept of differential cryptanalysis.

(d) Illustrate the concept of Chinese Remainder Theorem. By using Chinese Remainder Theorem solve the simultaneous congruence X ≡ 2 mod P for all P € {3, 5, 7}

(e) Use primality testing algorithm to check whether n = 221 is a prime.

(f) Explain random number generation techniques?

2. Answer any four of the following : (5×4=20)

(a) Briefly define a Group, Ring and Field.

(b) Determine gcd (1970, 1066).

(c) Explain Fermat's theorem. What is Euler's totient?

(d) Find all primitive roots of 25.

(e) Perform encryption and decryption, using RSA algorithm for P=3; q=11; e=7; M=5.

(f) Explain Diffie-Hellman key exchange algorithm. What is an elliptic curve?

3. Answer any two of the following: (10×2=20)

(a) What is a message authentication code? What characteristics are needed in a secure hash function?

(b) What is difference between Direct and Arbitrated digital signatures? Explain digital signature algorithm.

(c) What basic arithmetical and logical functions are used in MD5? Explain SHA-1 logic. Give comparison of SHA-1 and MD5.

4. Answer any two of the following : (10×2=20)

(a) What is the birthday attack problem? Explain with suitable examples.

(b) Discuss the roles of Whirlpool and ECDSA in cryptography system.

(c) Write short note on

(i) HMAC

(ii) CMAC

5. Answer any two of the following : (10×2=20)

(a) What do mean by finite automata? What are roles of finite automata in ciphers security with suitable example?

(b) Discuss the procedure of Cipher Design using automata with example?

(c) Discuss the followings:

(i) Structure of Ciphers

(ii) Selection of the Ma, h, and g function

*****