Printed Pages: 3 **MCAE-14**

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

Paper ID : 214459 **Roll No.** □□□□□□□□□□

M.C.A.

Theory Examination (Semester-IV) 2015-16

CRYPTOGRAPHY AND NETWORK SECURITY

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

Note:- Attempt all questions.

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

(a) What are the different factors on which Cryptography depends? Discuss in detail.

(b) Compute the value of 5^{17} mod 11 & 11^{17} mod 5.

(c) Explain Finite field of the form GF (p) & GF (2^n) with suitable example.

(d) What is Linear Congrurential Generator? Let m = 10, a =5, c = 14 and X_0 = 107 then find 5 a series of 5 random numbers.

(e) Find Euler's Totient number $\phi(88)$, $\phi(13)$.

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

(a) Discuss X.509 digital certificate format. What is its significance in cryptography?

(b) Discuss all the steps of PGP with suitable diagram.

(c) How E-Mail security is achieved? Discuss S/MIME with suitable block diagram.

(d) Discuss the SSL in detail.

(e) Write short note on the following:

i. SET

ii. Intrusion Detection

iii. Firewall

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

(a) Why Message Authentication is required? Discuss working of MAC with suitable block diagram. Also discuss HMAC & CMAC in detail.

(b) What is Hash Function? Discuss SHA 512 with all required steps, round function & block diagram.

(c) Discuss MD 5 Algorithm with all required steps and suitable block diagram.

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

(a) Discuss Public Key Cryptosystem. Explain RSA algorithm with suitable steps. Let p= 17, q=11, e=7 and d=23. Calculate the public key & private key and show encryption and decryption for plain text M= 88 by using RSA algorithm.

(b) Discuss Block Cipher Mode of Operations. Explain Data Encryption Standard Algorithm with suitable block diagram.

(c) What is Cryptanalysis? Discuss Linear and Differential cryptanalysis. Also discuss encryption decryption process of Advanced Encryption Standard Algorithm

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

(a) Explain digital Signature & Digital Signature Algorithm.

(b) Discuss Diffie Hellman key exchange method in detail. Let q = 353 , α = 3, X_A = 97 and X_B = 233. Then Compute $Y_{A,}$ $Y_{B,}$ K_A & K_B using Diffie Hellman.

(c) What do you understand by Chinese Remainder Theorem? Solve the following congruents by Chinese remainder theorem:

i. $x \equiv 2 \bmod 3$

ii. $x \equiv 3 \bmod 5$