Printed Pages : 1 Roll No. ECS084

B.TECH.

THEORY EXAMINATION (SEM–VIII) 2016-17

CRYPTOGRAPHY & NETWORK SECURITY

Time : 3 Hours *Max. Marks : 100*

Note : *Be precise in your answer. In case of numerical problem assume data wherever not provided.*

SECTION – A

1. Attempt the following: **10 x 2 = 20**

(a) What is Security Attacks? Discuss its types.

(b) Find gcd (1970, 1066) using Euclid's algorithm.

(c) Explain in brief Symmetric and Asymmetric Cryptography.

(d) State the Fermat's theorem.

(e) What is Replay Attack?

(f) Differentiate between Substitution & Transposition Cipher?

(g) What is Steganography?

(h) Define Finite Field in form of GF (p).

(i) Find the value of $\phi(12)$

(j) Discuss Triple DES?

SECTION – B

2. Attempt any five of the following questions: **5 x 10 = 50**

(a) Using Fermat's theorem, find the value of $3^{201} \bmod 11$.

(b) Discuss Group, Ring and Field.

(c) Discuss the design of S-Box of AES. How it differs from the S-Boxes of DES.

(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) What do you understand by Chinese Remainder Theorem? Solve by Chinese Remainder Theorem:

(i) $X \equiv 2 \bmod 3$

(ii) $X \equiv 3 \bmod 5$

(f) What are the requirements of Message Authentication Code (MAC)? Explain HMAC in detail with block diagram.

(g) Discuss Public Key Cryptosystem. Also 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

(h) Explain MD5 Message Digest Algorithm in detail with suitable steps and block diagram.

SECTION – C

Attempt any two of the following questions: **2 x 15 = 30**

3 What is Digital Certificate? Discuss the X.509 Digital Certificate Format. Also explain the Revocation of X.509 Digital Certificate.

4 What is Kerberos? Discuss Kerberos Version 4 in detail. Also differentiate it with Version 5.

5 **Write short notes on following:**

(i) Firewall

(ii) SSL

(iii) S/MIME