Code No: **R41051**

R10

Set No. 1

IV B.Tech I Semester Supplementary Examinations, Mar/April - 2016

CRYPTOGRAPHY AND NETWORK SECURITY

(Common to Computer Science & Engineering and Information Technology)

Time: 3 hours **Max. Marks: 75**

Answer any FIVE Questions
All Questions carry equal marks
****

1 a) What is a security attack? Explain different security mechanism. [8]

b) Explain the characteristics of block and stream ciphers. [7]

2 Explain AES encryption and Decryption in detail. [15]

3 a) State and prove Chinese remainder theorem. [8]

b) Using CRT, solve for x for the following
$x \equiv 2 \pmod 3$; $x \equiv 3 \pmod 5$; $x \equiv 2 (\mathrm{mod}\ 7)$ [7]

4 a) Explain the Diffie-Hellman key exchange algorithm. [7]

b) Consider a Diffie-Hellman scheme with a common prime q = 11 and a primitive root $\alpha = 2$

i) Show that 2 is primitive root of 11

ii) If user A has public key $Y_A = 9$, what is A's private key X_A?

iii) If user B has public key $Y_B = 3$, What is the shared secrete key K, shared with A [8]

5 a) What is message authentication? List the authentication requirements. [8]

b) Compare the principal characteristics of secure hash functions. [7]

6 a) Explain key management and distribution in detail. [7]

b) Explain X.509 directory authentication service. [8]

7 a) Explain ESP Header of IP Sec. [10]

b) Explain different Web security requirement. [5]

8 a) Explain Unix Password management. [7]

b) Explain Intrusion detection in detail. [8]

www.FirstRanker.com