Code No: **RT41051** **R13** **Set No. 1**

IV B.Tech I Semester Supplementary Examinations, March - 2017

CRYPTOGRAPHY AND NETWORK SECURITY

(Common to Computer Science & Engineering and Information Technology)

Time: 3 hours **Max. Marks: 70**

Question paper consists of Part-A and Part-B
Answer ALL sub questions from Part-A
Answer any THREE questions from Part-B
*****

PART–A *(22 Marks)*

1. a) What is the difference between mono alphabetic and poly alphabetic cipher? [4]
   b) Discuss the design principles of block cipher technique? [3]
   c) Explain the Fermat's theorem? [4]
   d) What are the properties of hashing functions? [4]
   e) What is e-mail security? Explain the technique for e-mail security? [4]
   f) Differentiate between tunnel mode and transport mode of IPSec. [3]

PART–B *(3x16 = 48 Marks)*

2. a) Breifly explain the security services and mechanisms defined under X800 standard. [8]
   b) Explain the UDP session hijacking in brief? [8]

3. Explain Data Encryption standard (DES) in detail. [16]

4. a) Briefly explain the Diffie Hellman Key Exchange algorithm? [8]
   b) Explain the Chinese remainder theorem with an example? [8]

5. Briefly explain the different message authentication functions with neat diagrams? [16]

6. Explain Secure socket layer in details? [16]

7. a) What is IDS? Explain the profile based IDS? [8]
   b) Briefly explain Encapsulating IP Security Payload? [8]