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

IV B.Tech I Semester Supplementary Examinations, February/March - 2018

CRYPTOGRAPHY AND NETWORK SECURITY

(Common to Computer Science and 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 meant by Fabrication? [3]
   b) What are Confusion and Diffusion properties of Modern Ciphers? [4]
   c) What is addition, multiplication and multiplicative and additive inverses modulo 8? [4]
   d) What is one way property, weak and strong collision resistance? [4]
   e) What is replay attack? What is the counter measure for it? [4]
   f) Define Base Rate Fallacy. [3]

PART–B *(3x16 = 48 Marks)*

2. a) Enumerate the security mechanisms defined by X.800. Explain each. [8]
   b) How are legitimate websites compromised with SQL injections, Malicious Advertisements? Explain. [8]

3. a) Which four tasks are performed in each round of AES Cipher? Explain. [12]
   b) Explain the Key Expansion process in AES. [4]

4. a) How is GCD calculated with Euclid's algorithm? Calculate the GCD of (270, 192) [8]
   b) Illustrate ElGamal Encryption and decryption algorithm. [8]

5. Illustrate Secure Hash algorithm in brief. [16]

6. a) Give an overview of Kerberos 4 dialogue. [8]
   b) What are the environmental shortcomings of Kerberos4? How does Kerberos 5 address them? [8]

7. a) How is Audit record analysis performed? [8]
   b) How are security associations combined? [8]