Code No: **RT4104E** **R13** **Set No. 1**

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

NETWORKS SECURITY AND CRYPTOGRAPHY

(Electronics and Communication Engineering)

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) Define Threat and Attack & What are the types of attacks on encrypted message. [4]
   b) What is the block size in DES? What is the cipher key size in DES? What is the round key size in DES? [4]
   c) Find the results of the following using Fermat's theorem:
   (i) 5^{15} mod 13 (ii) 15^{18} mod 17 [4]
   d) Define weak collision property of a hash function. [4]
   e) Draw the general format for PGP message. [3]
   f) List down the four phases of virus. [3]

PART–B *(3x16 = 48 Marks)*

2. a) Discuss the following:
   i. ARP attacks, route table modification
   ii. Buffer overflow & format string vulnerabilities [8]
   b) Explain the various types of cryptanalytic attacks. [8]

3. a) Explain the Key generation process in data encryption standard (DES) algorithm. [8]
   b) Explain the generation sub key and S Box from the given 32-bit key by Blowfish. [8]

4. a) Discuss clearly about fermat and Eluer's theorem with example. [8]
   b) Perform encryption and decryption using RSA Algorithm with the given P=5; q=13; e=19; M=6. [8]

5. a) Discuss clearly about the objectives of HMAC and it security features. [8]
   b) Write and explain the digital signature algorithm. [8]

6. a) Explain how PGP provides authentication and confidentiality for email services and for the transfer applications. [8]
   b) Discuss about the SSL architecture. [8]

7. a) Discuss about encapsulating security payload of IP. [8]
   b) Explain the types of Host based intrusion detection. List any two IDS software available. [8]