Code No: **R1641051** **R16** **Set No. 1**

IV B.Tech I Semester Regular/Supplementary Examinations, Jan/Feb - 2022

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 FOUR questions from Part-B
*****

PART–A *(14 Marks)*

1. a) State two facts of Euclidean algorithm. [2]
   b) Distinguish between diffusion and confusion. [2]
   c) Define the Chinese reminder theorem and its applications. [3]
   d) List the security services provided by a digital signature. [2]
   e) Draw the figure of MIME header. [3]
   f) What is transport mode and tunnel mode in IPsec? [2]

PART–B *(4x14 = 56 Marks)*

2. a) Outline the security services and the mechanisms to implement the services provided by ITU-T(X.800). [7]
   b) i) Write the algorithm for Extended Euclidean Algorithm (EEA). [4]
   ii) Given a=161 and b=28, find the gcd(a,b) and the values of s and t using EEA. [3]

3. a) Do Addition and subtraction are the same operations in polynomials? If yes, justify your answer by finding the result of $(x^5 + x^2 + x) * (x^7+x^4+x^3+x^2+x)$ in GF(2^8) with irreducible polynomial $(x^8+x^4+x^3+x+1)$. (Note that we use symbol * to show the multiplication of two polynomials) [7]
   b) Is Each round of Data Encryption Standard (DES) a Feistel Cipher? Explain in detail about DES algorithm. [7]

4. a) Define
   i) Euler's Phi-Function [2]
   ii) Fermat's Little Theorem [2]
   iii) Euler's Theorem [3]

   b) Why trapdoor one-way function is the key concept for asymmetric-key cryptography? Explain in detail by writing an algorithm for any one of the (RSA/Rabin/ELGamal/ECC) asymmetric-key cryptosystem. [7]

Code No: **R1641051** **R16** **Set No. 1**

5. a) Define hash function? List the variants in SHA by explaining SHA-512 in detail. [7]
   b) i) How does a man-in-the middle attack affect the Diffie–Hellman key exchange protocol? Explain [3]
   ii) Two users A and B want to establish a secret key using the Diffie–Hellman key exchange protocol using p = 23, g = 7, x = 3 and y = 6. Find the values of A and B and the secret key. [4]

6. a) List the protocols that provide security services to email and write in detail about any one of the protocol listed above. [7]
   b) Discuss how Secure Socket Layer plays an important role in web security? [7]

7. a) Draw the figures of Authentication header (AH) and Encapsulating Security Payload (ESP) header and trailer. [7]
   b) What are Intrusion Detection Systems? Explain the techniques used for Intrusion Detection Systems. [7]