(Pages : 2) **B – 2924**

Reg. No. : .....

Name : .....

Second Semester M.Tech. Degree Examination, December 2016
Electronics and Communication Engineering
Stream : Telecommunication Engineering
(2013 Scheme)
TTE 2002 : SECURE COMMUNICATION ENGINEERING

Time: 3 Hours Max. Marks : 60

Instructions: *Answer **any 2** questions from **each** Module.*
***Each** carries **10** marks.*

MODULE – I

1 a) Prove that if p is a prime, then every prime divisor of $2^p - 1$ is greater than p. **5**

b) Show that $\left(\frac{105}{131}\right) = 1$ and solve $x^2 \equiv 105 \pmod{131}$. **5**

2. a) Solve $25x + 95y = 970$. **5**

b) If p is a prime and n is an integer such that $p|(4n^2 + 1)$, then prove that $p \equiv 1 \pmod 4$. **5**

3. a) Assume that an element x of a group has order rs. Find the order of x^r. **5**

b) Consider a finite group of n elements. Prove that n is divisible by the order of every element of that group. **5**

MODULE – II

4. A shift cipher key is exchanged using the Diffie-Hellman method with g = 5 and p = 47. The actual numbers exchanged were X = 38 and Y = 3. **10**

i) Find the key.

ii) Using the key in the previous exercise, decipher the message :

EQPITCVWNCVKQPU.

P.T.O.

5. Consider the Knapsack crypto system with modulus m = 701, u = 200 and the following super-increasing sequence : **10**

   (1, 4, 9, 25, 41, 82, 170, 333)

   i) Determine the public key

   ii) Encrypt message 10010101 and decrypt the result.

6. A message is encrypted with RSA using n = 247 and e = 31. The encrypted message reads 045 199 106 219. What is the original message ? **10**

MODULE – III

7. a) Prove that discrete logarithms in a cyclic group of order N can be computed in less than $2\left[\sqrt{N}\right]$ operations. **5**

   b) Factorize 809009 using Fermat's factorization method. **5**

8. a) Show that $56^{100} \equiv 1 \pmod 5$. **5**

   b) Show that if p is prime and $2^p - 1$ is composite, then $2^p - 1$ is pseudoprime to the base 2. **5**

9. a) If n is an odd pseudoprime, then show that $N = 2^n - 1$ is also an odd pseudoprime. **6**

   b) Compute the discrete logarithm of h = 15 with respect to g = 2 modulo p = 29. **4**