Model Question Paper

Second Semester M. Tech Degree Examination in
Electronics and Communication Engineering
Stream: Telecommunication Engineering (2013 Scheme)

TTE 2002: Secure Communication

Time : 3 hours Max. Marks : 60

Instructions: *Answer any 2 questions from each module (Each Carries 10 Marks)*

Module I

1. (a) Explain in detail about the characteristics of different complexity classes. (10)
2. (a) State Fermat's theorem. Using this theorem find

   i) $60^{-1} \bmod 101$ ii) $3^{12} \bmod 11$ (5)

   (b) Explain Euler's theorem and find the values of

   i) $20^{62} \bmod 77$ ii) $71^{-1} \bmod 100$ (5)
3. (a)Discuss about quadratic residues and solve $3y^2+5y+9 \equiv 0 \pmod{11}$ (6)

   (b) Solve the linear Diophantine equation $21x+14y=35$ (4)

Module II

4. (a) Generate a PN sequence using a 5 stage LFSR. Check for randomness. Discuss about the use of random numbers in cryptography. (6)

   (b) Explain about message digest scheme MD5. (4)
5. (a) What are the requirements of a hash function? Explain in detail about hash functions. (6)

   (b) In a public key system using RSA, assume that an intruder intercept the cipher text c=10 sent to a user whose public key is e=5, n=35. What is the plain text m? (4)
6. Explain how encryption and decryption are performed in AES standard. Also explain how the key expansion is performed in AES. (10)

Module III

7. Explain Baby step- Giant step algorithm for computing discrete logarithm. Find the value of x where $5^x = 9$ in Z^*_{14} (10)
8. Discuss about different primality tests in cryptanalysis. (10)
9. (a) Explain different factorization methods. (6)
   (b) Does the number 561 pass the Fermat's test? (4)