Second Semester M. Tech Degree Examination in

Electronics and Communication Engineering

Stream: Telecommunication Engineering (2013 Scheme)

TTE 2002 SECURE COMMUNICATION

MODEL QUESTION PAPER

Time: 3 hours Max. Marks: 60

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

Module I

1. State and prove Fermat's little theorem.
2. Let p denote a prime, then prove that $x^2 \equiv -1$ has solutions if and only if p=2 or p=1 (mod 4).
3. Solve the congruences (i) $x^3+2x-3\equiv0$ (mod 9) (ii) $x^3+2x-3\equiv0$(mod 5).

Module II

4. Assume that two users want to establish a common secretkey over an insecure channel by using Diffie-Hellman key exchange protocol.The private key for user A is 11 and for user B is 14. Consider a commonlyknown prime 17.

   (i)Find the smallest primitive element for p = 17.

   (ii) Obtain the common key by using the primitive element found above.
5. Explain Data Encryption Standard.
6. Show that any sequence of positive integers $\{v_i\}$ with $v_{i+1} \geq 2v_i$ for all i is super increasing.

Module III

7. Find all bases b for which 15 is a pseudoprime.
8. Prove that 561 is the smallest Carmichael number.
9. Let n=4633. Find the smallest factor base B such that the squares of 68, 69 and 96 are B numbers and then factor 4633.