APJ ABDUL KALAM TECHNOLOGICAL UNIVERSITY

THIRD SEMESTER M. TECH DEGREE EXAMINATION

Electronics & Communication Engineering

(Telecommunication Engineering)

04EC7803—Secure Communication

Max. Marks: 60 Duration: 3 Hours

PART A

Answer All Questions

Each question carries 3 marks

1. Determine 5^{15} mod 13 using Fermat's little theorem.
2. Find the multiplicative inverse of 11 in $Z_{26?}$
3. Draw a PN sequence generator with feedback connection governed by the equation

$$1+x+x^2+ x^4$$

4. Explain El Gamal's public key cryptosystem with a suitable example.
5. What is primality testing? List the different algorithms for primality testing.
6. Check the primality for n= 61 using strong pseudo primality test.
7. Discuss on Fermat's factoring algorithm for integer factorization.
8. Compute x in $5^x \equiv 7$ mod 23 using Shank's Baby Step Giant step algorithm.

PART B

Each question carries 6 marks

9. Solve the equation $x^2-5x+6 \equiv 0 \pmod{11}$**.**

OR

10. Describe Legendre symbol and its properties.
11. Differentiate Group, Ring and Field with examples.

OR

12. Explain with an example Extended Euclidean algorithm.
13. Explain with a neat schematic the concept of public key cryptography

OR

14. Discuss briefly the on the need and concept of Hash functions in message authentication.
15. Elaborate on the concept of Digital Signature with neat diagram.

OR

16. Write in detail on DES encryption standard with neat schematic.
17. Discuss in detail on modular exponentiation and compute 3^{200} mod 50.

OR

18. Write in detail on the fast group operations on elliptic curves and determine 105P.
19. Illustrate and explain trial division algorithm for integer factorization.

OR

20. Discuss in detail on the algorithm for elliptic curve discrete logarithm.