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. Describe the relationship between the different complexity classes.
2. Find 6^{24} mod 35 using Euler's theorem.
3. Use the Affine cipher to encrypt the message "cryptography" with the key pair (7, 2).
4. Write a brief note on substitute byte transformation in DES encryption standard.
5. Check the primality for n= 61 using strong pseudo primality test.
6. Write a brief note on fast modular exponentiation.
7. Illustrate Fermat's factoring algorithm for integer factorization.
8. Compute x in $3^x \equiv 19 \bmod 59$ using Shank's Baby Step Giant step algorithm.

PART B

Each question carries 6 marks

9. Determine 2^{50} mod 17 using Wilson's theorem.

OR

10. Detail the concept of asymmetric key cryptography with a neat schematic.

11. What is a commutative group and discuss its properties.

OR

12. Calculate the multiplicative inverse of 8 in Z_{10}?

13. Elaborate on the deciphering process of a cipher text using Hill Cipher taking a suitable example.

OR

14. Explain the different types of message authentication systems.
15. Elaborate on the concept of Digital Signature with neat diagram.

OR

16. Describe RSA algorithm and perform the same choosing 17 and 11 as prime numbers to start with.

17. Explain in detail on the fast group operations on elliptic curves with an example.

OR

18. Discuss briefly on Fermat's Pseudo primality test with suitable illustration.
19. Illustrate and explain any one integer factorization algorithm and factorize n=10541.

OR

20. Discuss in detail on discrete logarithm and describe the algorithm of index calculus for elliptic curve discrete logarithm problem.