**[Mar-21]**

# [19ECS707]
# M.Tech. Degree Examination

## I Semester
## Cyber Forensics And Information Security (CFIS)

## NUMBER THEORY AND CRYPTOGRAPHY

(For the admitted batch 2019-20 onwards)

**Time: 3 Hours** **Max.Marks: 60**

---

**Instructions:** All parts of the unit must be answered in one place only.
Figures in the right hand margin indicate marks allotted.

---

## SECTION-A

1. **Answer All the Questions:** **10x2=20M**

   a. The solution of $25x \equiv 15 (\mathrm{mod} 29)$ is.

   b. Compute the value of $\phi(37)$.

   c. What are symmetric and asymmetric key systems?

   d. For the given formula, 17*x=1 mod 5, find out the value of x.

   e. In public key cryptosystem which keys are kept as public.

   f. If Richard wants to send an encrypted message to Sue using a public key cryptosystem, which key does he use to encrypt the message.

   g. Give an example of prime factorization of a given number.

   h. Justify your answer why miller rabin primality test produces accurate results compared to other techniques?

   i. Give an equation of an elliptic curve over finite field.

   j. A point G over an elliptic curve over finite field can be multiplied by integer K and the result is another point p that lies on -----curve.

## Section-B

**Answer the following** **5x8=40M**

### UNIT-I

2. State and describe Euler’s theorem and Fermat’s theorem. 8

**OR**

3. Find all the quadratic residues of 13. 8

## UNIT-II

4. State block cipher design principles, and explain Fiestal structure with the help of block diagram. 8

**OR**

5. Give a brief note on Linear and differential cryptanalysis. 8

## UNIT-III

6. Explain in steps clearly, any one of the methods which is used to solve discrete log problem. 8

**OR**

7. State Discrete Log Problem and solve 3^x≡7(mod 19). 8

## UNIT-IV

8. Describe Miller-Rabin primality testing and explain briefly with help of an example. 8

**OR**

9. Check 1729 is pseudo prime or not. Justify your answer. 8

## UNIT-V

10. Give a brief note on elliptic curve point addition and explain with help of an example. 8

**OR**

11. Given an elliptic curve over Fp(17) with a= 0 and b= 7. Show that the points(5,8),(9,15) belongs to the curve. If yes, justify your answer. 8