CRYPTOGRAPHY

Duration : 30 Hours	Exam Marks : 50

Course Description:

Cryptography is the science of encrypting and decrypting any information this is one of the finest application of number Theory in this course, the fundamentals of cryptography are dealt with. As a piece of information is expressed through symbols, representing it in a way that only the intended party would know it is the best part of encryption and decryption. As the world is flooded with information, generation, transfer and acquisition of it is very important. Students with basic background in Number Theory can take up the course.

This course is concerned with the basic of analytical number theory. Topics such as divisibility, congruence's quadratic residues and functions of number theory are covered in this course. An introduction to Cryptography is also included.

Course Outcome:

On successful completion of the course, the students should be able to

- Define and interpret the concepts of divisibility, congruence, greatest common divisor, prime, and prime-factorization.
- Solve congruences types, and use the theory of congruences in application
- Prove and apply properties of multiplicative functions such as the Euler phi-function and of quadratic residues.
- Apply the Law of Quadratic Reciprocity and other methods to classify numbers as primitive roots, quadratic residues, and quadratic non-residues.
- Produce rigorous arguments (proofs) centered on the material number theory.
- Encrypting and Decrypting messages.

Module I: Divisibility	**14Hours**

Level of knowledge-Focus: Basic, conceptual and analytical

The Euclidian division algorithms, The Greatest Common Divisor, The Euclidean G.C.D of integers and polynomials, Prime and Composite numbers.

Basic Properties of Congruence, Complete residue system modulo m, reduced residue system modulo m, Euler's φ function, Fermat's theorem, Euler's generalization of Fermat's theorem, The chinese reminder theorem.

Module II:Algebraic Structure, Quadratic residues and Some function of number theoretic-functions	**06Hours**

Algebraic –Structures-Multiplicative groups, Cyclic groups, primitive roots modn, Finite fields, Legendre symbol, arithmetic functions, the Mobius inversion formula, Problems.

Module III:Introduction to Cryptography (self learning module)	**10Hours**

Public key Cryptography , RSA Public key Crypto system, Elgamal Public key Crypto system, Diffie Hellman key Exchange, The Knapsack Cryptosystem, crypt Analysis : Hard number theoretic problems-Integer factoring.

Reference Books:

1. Lvan Niven, Herbert S.Zuckerman and Hugh L. Montgomery, An introduction to the theory of numbers, john Willey 2004.
2. David M.Burton, Elementary Number Theory, 15th Ed. Tata McGraw-Hill, 2016

3. Neal Koblitz, A course in number theory and cryptography, Reprint: Springer, 2010
4. Lvan Niven, Herbert S.Zuckerman and Hugh L.Montogomery, An introduction to the theory of numbers,John Wiley, 2004
5. Computational Number : Theory-Abhijit Das.
6. Public key Cryptography: Theory and Practice-Abijit Das and C.E. Veni Madhavan.
7. Public key Cryptography : Theory and Practice, Parson Education India, 2009
8. Applied Cryptography –B, Schneier.
9. Computers and Network Security-W.Stallings .