DEPARTMENT OF COMPUTER ENGINEERING

Subject Code: 10CE0101

Subject Name: Mathematical Foundations for Cyber Security

M.Tech. Year - I

Objective: Students are expected to learn basics maths used for information security and to design and analyse security protocols. These concepts will help them to develop security model and analyse them before being used in many commercial, industrial as well as web application.

Credits Earned: 4 Credits

Course Outcomes: After completion of this course, student will be able to

- Effectively express the concepts and results of Number Theory.
- Understand basic concepts of various algebraic structures and theorems like Euler's theoerem for designing security algorithm.
- Understand coding theory which will be useful for data compression, information hiding
- Illustrate various pseudorandom number generation used for designing security protocols and for its analysis.

Pre-requisite of course: NA.

Teaching and Examination Scheme

Teaching Scheme (Hours)			Credits	Theory Marks			Tutorial/ Practical Marks		Total Marks
Theory	Tutorial	Practical		ESE (E)	Mid Sem (M)	Internal (I)	Viva (V)	Term work (TW)	
4	0		4	50	30	20	00	25	125

Contents

Unit	Topics	Contact Hours
1	**NUMBER THEORY**: Introduction - Divisibility - Greatest common divisor - Prime numbers - Fundamental theorem of arithmetic - Mersenne primes - Fermat numbers - Euclidean algorithm - Fermat's theorem - Euler totient function - Euler's theoerem. Congruences: Definition - Basic properties of congruences - Residue classes - Chinese remainder theorem	8
2	**ALGEBRAIC STRUCTURES**: Groups – Cyclic groups, Cosets, Modulo groups - Primitive roots - Discrete logarithms. Rings – Sub rings, ideals and quotient rings, Integral domains. Fields – Finite fields – GF (p^n), GF(2^n) - Classification - Structure of finite fields. Lattice, Lattice as Algebraic system, sub lattices, some special lattices.	9
3	**PROBABILITY THEORY**: Introduction – Concepts of Probability - Conditional Probability - Baye's Theorem - Random Variables – discrete and continuous- central Limit Theorem-Stochastic ProcessMarkov Chain.	6
4	**CODING THEORY**: Introduction - Basic concepts: codes, minimum distance, equivalence of codes, Linear codes - Linear codes - Generator matrices and parity-check matrices - Syndrome decoding – Hamming codes - Hadamard Code - Goppa codes	9
5	**PSEUDORANDOM NUMBER GENERATION**: Introduction and examples - Indistinguishability of Probability Distributions - Next Bit Predictors - The Blum-Blum-Shub Generator – Security of the BBS Generator.	8
	Total Hours	**40**

References:

1. 1. D. S. Malik, J. Mordeson, M. K. Sen, Fundamentals of abstract algebra, Tata McGraw Hill

2. P. K. Saikia, Linear algebra, Pearson Education, 2009.

3. I. Niven, H.S. Zuckerman and H. L. Montgomery, An introduction to the theory of numbers, John Wiley and Sons, 2004.

4. D P Bersekas and J N Tsitsiklis, Introduction to probability, Athena Scientific, 2008

5. Douglas Stinson, 'Cryptography – Theory and Practice', CRC Press, 2006.

6. Sheldon M Ross, "Introduction to Probability Models", Academic Press, 2003.

7. C.L. Liu, 'Elements of Discrete mathematics', McGraw Hill, 2008.

8. Fraleigh J. B., 'A first course in abstract algebra', Narosa, 1990.

9. Joseph A. Gallian, ''Contemporary Abstract Algebra', Narosa, 1998

Suggested Theory distribution:

The suggested theory distribution as per Bloom's taxonomy is as per follows. This distribution serves as guidelines for teachers and students to achieve effective teaching-learning process

Distribution of Theory for course delivery and evaluation					
Remember	Understand	Apply	Analyze	Evaluate	Create
5%	10%	15%	30%	20%	30%

Instructional Method:

a. The course delivery method will depend upon the requirement of content and need of students. The teacher in addition to conventional teaching method by black board, may also use any of tools such as demonstration, role play, Quiz, brainstorming, MOOCs etc.

b. The internal evaluation will be done on the basis of continuous evaluation of students in the laboratory and class-room.

c. Practical examination will be conducted at the end of semester for evaluation of performance of students in laboratory.

d. Students will use supplementary resources such as online videos, NPTEL videos, e-courses, Virtual Laboratory

Supplementary Resources:

1. https://ocw.mit.edu/courses/mathematics/
2. http://homes.soic.indiana.edu/yh33/Teaching/I231-2016/syllabus.html
3. http://nptel.ac.in/syllabus/106105031/
4. http://nptel.ac.in/syllabus/syllabus_pdf/106105031.pdf
5. http://nptel.ac.in/syllabus/106101004/
6. https://eliademy.com/catalog/physical-science/elementary-number-theory.html