राष्ट्रीय प्रौद्योगिकी संस्थान पटना / NATIONAL INSTITUE OF TECHNOLOGY PATNA
संगणक विज्ञान एंव अभियांत्रिकी विभाग / DEPARTMENT OF COMPUTER SCIENCE AND ENGINEERING
अशोक राजपथ, पटना-८००००५, बिहार / ASHOK RAJPATH, PATNA-800005, BIHAR
Phone No.: 0612-2372715, 2370419, 2370843, 2371929 Ext- 200, 202 Fax-0612-2670631 Website: www.nitp.ac.in

No:- Date:

CSXX2835: Mathematical Foundation for Information Security

L-T-P-Cr: 3-0-0-3

Pre-requisites: None

Objectives:

- To study mathematical foundations necessary for Information Security and related fields
- To know about how Security problems can be formulated with mathematical models
- To have the necessary core skills of mathematically analyzing Information Security in real world problems

Course Outcomes:
At the end of the course, a student should have:

Sl. No.	Outcome	Mapping to POs
1.	Understood the knowledge of basic mathematics related to research in networks	PO1, PO2
2.	Become proficient in applying the mathematics related to network in their projects and seminars	PO1, PO3
3.	Become capable of applying concepts related to graphs for network optimization	PO2, PO3

UNIT I: Introduction: **Lectures: 3**
Logic, Mathematical reasoning, Sets, Basics of counting, Relations.

UNIT II: Graph Theory: **Lectures: 10**
Euler graphs, Hamiltonian paths and circuits, planar graphs, trees, rooted and binary trees, distance and centres in a tree, fundamental circuits and cut sets, graph colorings and applications, chromatic number, chromatic partitioning, chromatic polynomial, matching, vector spaces of a graph.

UNIT III: Analytic Number Theory: **Lectures: 10**
Euclid's lemma, Euclidean algorithm, basic properties of congruences, residue classes and complete residue systems, Euler-Fermat theorem, Lagrange's theorem and its applications, Chinese remainder theorem, primitive roots.

UNIT IV: Algebra: **Lectures: 4**
Groups, cyclic groups, rings, fields, finite fields and their applications to cryptography.

UNIT V: Linear Algebra: **Lectures: 4**

Vector spaces and subspaces, linear independence, basis and dimensions, linear transformations andapplications.

UNIT VI: Probability and Statistics: **Lectures: 10**

Introduction to probability concepts, random variables, probability distributions (continuous and discrete), Bayesian approach to distributions, mean and variance of a distribution, joint probability distributions, theory of estimation, Bayesian methods of estimation.

UNIT VII: Random Processes: **Lectures: 5**

General concepts, power spectrum, discrete-time processes, random walks and other applications, Markov chains, transition probabilities.

Text Books:

1. R.P.Grimaldi, "*Discrete and Combinatorial Mathematics*", Pearson Education, Fifth edition, 2007.
2. K. H. Rosen, "*Discrete Mathematics and its applications*", Tata MCGraw-Hill Publishing company limited, New Delhi, 7th edition, 2007.
3. H. Anton, "*Elementary Linear Algebra*", John Wiley & Sons, 2010.
4. N. Deo, "*Graph theory with applications to Engineering and Computer Science*", Prentice Hall of India, New Delhi, 1974.
5. T. M. Apostol, "*Introduction to Analytic Number Theory*", Springer, 1976.
6. Douglas C. Montgomery and George C. Runger, "*Applied Statistics and Probability for Engineers*", Third Edition, John Wiley & Sons Inc., 2003.
7. A. Papoulis and U. Pillai, Probability, "*Random Variables and Stochastic Processes*", 4th Edition, McGraw Hill, 2002.
8. Ronald E. Walpole, Raymond H Myres, Sharon.L.Myres and Kying Ye, "*Probability and Statistics for Engineers and Scientists*", 7th Edition, Pearson Education, 2002.