MATHEMATICAL FOUNDATION FOR CYBER SECURITY

III Semester: CSE(CS)

<table>
<thead>
<tr>
<th>Course Code</th>
<th>Category</th>
<th>Hours / Week</th>
<th>Credits</th>
<th>Maximum Marks</th>
</tr>
</thead>
<tbody>
<tr>
<td>ACCC01</td>
<td>Core</td>
<td>L T P C CIA SEE Total</td>
<td>3 1 0 4 30 70 100</td>
<td></td>
</tr>
</tbody>
</table>

Contact Classes: 45  Tutorial Classes: 15  Practical Classes: Nil  Total Classes: 60

Prerequisites: There are no prerequisites to take this course.

COURSE OVERVIEW:

This course presents mathematical concepts in cyber security domain. The cryptography is widely used to secure data against eavesdropping. The cryptographic algorithms are based on mathematical algorithms where these algorithms use the secret key for a secure transformation of data. Number theory, coding theory and cryptography are well-known areas of information security as both are necessary for today's technology oriented; online-based world. Essentially, coding theory is associated with error correcting codes. Cyber security studies will require a strong math background. Strong analytics and statistical analysis skills needed. Encryption and programming will go hand in hand. Cyber security is a technical field and one that at its core, requires strong quantitative skills.

II. COURSE OBJECTIVES:

The students will try to learn:

I. The basics of mathematical models used in information security.
II. The general understanding of cyber security relationship with numbers
III. The security model and analyze them before being used in many commercial, industrial as well as web application.
IV. The role of mathematics in a complex system such as the Internet.

I. SYLLABUS:

MODULE – I: INTRODUCTION TO NUMBER THEORY (09)
Definition - Divisibility - Greatest common divisor - Prime numbers - Fundamental theorem of arithmetic - Mersenne primes - Fermat numbers - Euclidean algorithm - Fermat’s theorem - Euler totient function - Euler’s theorem. Congruences: Definition - Basic properties of congruences - Residue classes - Chinese remainder theorem.

MODULE – II: ALGEBRAIC STRUCTURE (09)
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(pn), GF(2n) - Classification - Structure of finite fields. Lattice, Lattice as Algebraic system, sub lattices, some special lattices.

MODULE – III: PROBABILITY THEORY (09)


MODULE - IV: CODING THEORY (09)

MODULE - V: PSEUDORANDOM NUMBER GENERATION (09)
Introduction and examples - Indistinguishability of Probability Distributions - Next Bit Predictors - The Blum-Blum-Shub Generator – Security of the BBS Generator.
IV. TEXT BOOKS:

V. REFERENCE BOOKS:

VI. WEB REFERENCES: