CS6701 CRYPTOGRAPHY AND NETWORK SECURITY

INTRODUCTION AND NUMBER THEORY

Unit I Overview

Unit Objectives

- Understand OSI security architecture and classical encryption techniques
- Acquire fundamental knowledge on the concepts of finite field and number theory

Unit Outcomes

- At the end of this session, students will be able to
  - Analyze various cryptographic techniques
  - Implement classical cryptographic systems

Course Outcomes Addressed

Unit Outcomes	Course Outcomes
UO1: Analyze various cryptographic techniques UO2: Implement classical cryptographic systems	• Compare various cryptographic techniques

References

1. William Stallings, Cryptography and Network Security, 6th Edition, Pearson Education, March 2013.
2. Charlie Kaufman, Radia Perlman and Mike Speciner, “Network Security”, Prentice Hall of India, 2002.