CS6701 CRYPTOGRAPHY AND NETWORK SECURITY

BLOCK CIPHERS & PUBLIC KEY CRYPTOGRAPHY

Unit II Overview

Unit Objectives

- Present an overview of DES
- Distinguish among groups, rings and fields
- Acquire fundamental knowledge on the concepts of finite fields and number theory
- Present an overview of the general structure of AES
- List and explain the requirements for a public key cryptosystem
- Present an overview of the RSA algorithm
- Define Diffie-Hellman key exchange
- Present an overview of ECC

Unit Outcomes

- At the end of this session, students will be able to
  - Analyze various private and public key cryptographic techniques
  - Implement DES and RSA
  - Understand Diffie-Hellman key exchange

Course Outcomes Addressed

Unit Outcomes	Course Outcomes
UO1: Analyze various private and public key cryptographic techniques UO2: Implement DES and RSA UO3: Understand Diffie-Hellman key exchange	• Design secure applications

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.