NPTEL Video Course - Computer Science and Engineering - NOC:Introduction to Cryptology

Subject Co-ordinator - Dr. Sugata Gangopadhyay

Co-ordinating Institute - IIT - Roorkee

Sub-Titles - Available / Unavailable | MP3 Audio Lectures - Available / Unavailable

Lecture 1 - Introduction Caeser cipher
Lecture 2 - Modular arithmetic, shift cipher
Lecture 3 - Affine Cipher, Vigenere Cipher
Lecture 4 - Prefect secrecy, Application of Shift Cipher
Lecture 5 - Problem Discussion on Affine cipher and Perfect Secrecy
Lecture 6 - Product Cipher, Block Cipher, Modes of Operation for Block Cipher
Lecture 7 - Substitution Permutation network, Fiestel Cipher
Lecture 8 - S-Box Theory
Lecture 9 - Cryptanalysis and its Variants, Linear Attack
Lecture 10 - Problem Discussion
Lecture 11 - Public Key Cryptology Introduction RSA Cryptosystem
Lecture 12 - Complexity analysis of Euclidian Algorithm and RSA Cryptosystem square and multiply algorithm
Lecture 13 - Primality testing
Lecture 14 - Efficien Computation of Jacobi Symbol Primality Testing
Lecture 15 - Problem Discussion on Jacobi Symbol Calculation and RSA Cryptosystem
Lecture 16 - Cryptographic hash function
Lecture 17 - Random Oracle model, Security of hash functions
Lecture 18 - Randomized Algorithm and its application on Preimage resistance and collision resistance
Lecture 19 - Iterated Hash Functions
Lecture 20 - Problem Discussionn