NPTEL Video Course - Computer Science and Engineering - NOC:Foundations of Cryptography

Subject Co-ordinator - Prof. Ashish Choudhury

Co-ordinating Institute - IIT - Madras

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

Lecture 1 - Introduction
Lecture 2 - Symmetric-key Encryption
Lecture 3 - Historical Ciphers and their Cryptanalysis
Lecture 4 - Perfect Security
Lecture 5 - Limitations of Perfect Security
Lecture 6 - Introduction to Computational Security
Lecture 7 - Semantic Security
Lecture 8 - Pseudo-random Generators (PRGs)
Lecture 9 - Operations on Pseudorandom Generators
Lecture 10 - Stream Ciphers
Lecture 11 - Provably-secure Instantiation of PRG
Lecture 12 - Practical Instantiations of PRG
Lecture 13 - CPA-security
Lecture 14 - Pseudo-random Functions (PRFs)
Lecture 15 - CPA-secure Encryption from PRF
Lecture 16 - Modes of Operations of Block Ciphers - Part I
Lecture 17 - Modes of Operations of Block Ciphers - Part II
Lecture 18 - Theoretical Constructions of Block Ciphers
Lecture 19 - Practical Constructions of Block Ciphers - Part I
Lecture 20 - Practical Constructions of Block Ciphers - Part II
Lecture 21 - From Passive to Active Adversary
Lecture 22 - Message Integrity and Authentication
Lecture 23 - Message Authentication for Long Messages - Part I
Lecture 24 - Message Authentication for Long Messages - Part II
Lecture 25 - Information-theoretic MACs - Part I
Lecture 26 - Information-theoretic MACs - Part II
Lecture 27 - Cryptographic Hash Functions - Part I
Lecture 28 - Cryptographic Hash Functions - Part II
Lecture 29 - Message Authentication Using Hash Functions

Lecture 30 - Generic Attacks on Hash Functions and Additional Applications of Hash Functions
Lecture 31 - Random Oracle Model - Part I
Lecture 32 - Random Oracle Model - Part II
Lecture 33 - Authenticated Encryption
Lecture 34 - Composing CPA-secure Cipher with a Secure MAC - Part I
Lecture 35 - Composing CPA-secure Cipher with a Secure MAC - Part II
Lecture 36 - Key-Exchange Protocols - Part I
Lecture 37 - Key-Exchange Protocols - Part II
Lecture 38 - Cyclic groups
Lecture 39 - Cryptographic Hardness Assumptions in the Cyclic Groups
Lecture 40 - Candidate Cyclic Groups for Cryptographic Purposes - Part I
Lecture 41 - Candidate Cyclic Groups for Cryptographic Purposes - Part II
Lecture 42 - Cryptographic Applications of the Discrete Log Assumption
Lecture 43 - Public-key Encryption
Lecture 44 - El Gamal Public-key Encryption Scheme
Lecture 45 - RSA Assumption
Lecture 46 - RSA Public-key Cryptosystem
Lecture 47 - Hybrid Public-key Cryptosystem
Lecture 48 - CCA-Secure Public-key Ciphers
Lecture 49 - CCA-Secure Public-key Ciphers Based on Diffie-Hellman Problems
Lecture 50 - CCA-Secure Public-key Ciphers Based on RSA Assumption
Lecture 51 - Digital Signatures
Lecture 52 - RSA Signatures
Lecture 53 - Identification Schemes
Lecture 54 - Schnorr Signature Scheme and TLS/SSL
Lecture 55 - Number Theory
Lecture 56 - Secret Sharing
Lecture 57 - Zero-Knowledge Protocols - Part I
Lecture 58 - Zero-Knowledge Protocols - Part II
Lecture 59 - Good Bye for Now