

NPTEL Video Lecture Topic List - Created by LinuXpert Systems, Chennai

NPTEL Video Course - Computer Science and Engineering - NOC:Cryptography And Network Security

Subject Co-ordinator - Prof. Sourav Mukhopadhyay

Co-ordinating Institute - IIT - Kharagpur

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

- Lecture 1 - Introduction to Cryptography
- Lecture 2 - Classical Cryptosystem
- Lecture 3 - Cryptanalysis on Substitution Cipher (Frequency Analysis)
- Lecture 4 - Play Fair Cipher
- Lecture 5 - Block Cipher
- Lecture 6 - Data Encryption Standard (DES)
- Lecture 7 - DES (Continued...)
- Lecture 8 - Triple DES and Modes of Operation
- Lecture 9 - Stream Cipher
- Lecture 10 - Pseudorandom Sequence
- Lecture 11 - LFSR Based StreamCipher
- Lecture 12 - Mathematical Background
- Lecture 13 - Abstract Algebra (Continued...)
- Lecture 14 - Number Theory
- Lecture 15 - Number Theory (Continued...)
- Lecture 16 - Modular Inverse
- Lecture 17 - Extended Euclidean Algorithm
- Lecture 18 - Fermat's Little Theorem, Euler Phi-Function
- Lecture 19 - Euler's theorem, Quadratic Residue
- Lecture 20 - Polynomial Arithmetic
- Lecture 21 - Advanced Encryption Standard (AES)
- Lecture 22 - Advanced Encryption Standard (AES) (Continued...)
- Lecture 23 - Introduction to Public Key Cryptosystem, Diffie-Hellman Key Exchange
- Lecture 24 - Knapsack Cryptosystem
- Lecture 25 - RSA Cryptosystem
- Lecture 26 - More on RSA
- Lecture 27 - Primarily Testing
- Lecture 28 - ElGamal Cryptosystem
- Lecture 29 - Elliptic Curve over the Reals

Get DIGIMAT For High-Speed Video Streaming of NPTEL and Educational Video Courses in LAN

<http://www.digimat.in>

NPTEL Video Lecture Topic List - Created by LinuXpert Systems, Chennai

- Lecture 30 - Elliptic curve Modulo a Prime
- Lecture 31 - Generalised ElGamal Public Key Cryptosystem
- Lecture 32 - Chinese Remainder Theorem
- Lecture 33 - Rabin Cryptosystem
- Lecture 34 - Legendre and Jacobi Symbol
- Lecture 35 - Jacobi Symbol (Continued...)
- Lecture 36 - Message Authentication
- Lecture 37 - Digital Signature
- Lecture 38 - Key Management
- Lecture 39 - Key Exchange
- Lecture 40 - Hash Function
- Lecture 41 - Universal Hashing
- Lecture 42 - Cryptographic Hash Function
- Lecture 43 - Secure Hash Algorithm (SHA)
- Lecture 44 - Digital Signature Standard (DSS)
- Lecture 45 - More on Key Exchange Protocol
- Lecture 46 - Cryptoanalysis
- Lecture 47 - Memory Trade off Attack
- Lecture 48 - Differential Cryptoanalysis
- Lecture 49 - More on Differential Cryptoanalysis
- Lecture 50 - Linear Cryptoanalysis
- Lecture 51 - Cryptoanalysis and Stream Cipher
- Lecture 52 - Modern Stream Cipher
- Lecture 53 - Shamir Secret Sharing
- Lecture 54 - Identity Based Encryption (IBE)
- Lecture 55 - Attribute Based Encryption
- Lecture 56 - Functional Encryption (Introduction)
- Lecture 57 - Discrete Logarithm Problem (DLP)
- Lecture 58 - Implementation Attacks
- Lecture 59 - The Secure Sockets layer (SSL)
- Lecture 60 - Pretty Good Privacy (PGP)