NPTEL Video Course - Computer Science and Engineering - Cryptography and Network Security

Subject Co-ordinator - Dr. Debdeep Mukhopadhyay

Co-ordinating Institute - IIT - Kharagpur

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

Lecture 1 - Introduction
Lecture 2 - Overview on Modern Cryptography
Lecture 3 - Introduction to Number Theory
Lecture 4 - Probability and Information Theory
Lecture 5 - Classical Cryptosystems
Lecture 6 - Cryptanalysis of Classical Ciphers
Lecture 7 - Shannons Theory
Lecture 8 - Shannons Theory (Continued...1)
Lecture 9 - Shannons Theory (Continued...2)
Lecture 10 - Symmetric Key Ciphers
Lecture 11 - Block Cipher Standards (DES)
Lecture 12 - Block Cipher Standards (AES)
Lecture 13 - Block Cipher Standards (AES) (Continued...)
Lecture 14 - Linear Cryptanalysis
Lecture 15 - Differential Cryptanalysis
Lecture 16 - Few other Cryptanalytic Techniques
Lecture 17 - Overview on S-Box Design Principles
Lecture 18 - Modes of Operation of Block Ciphers
Lecture 19 - Stream Ciphers
Lecture 20 - Stream Ciphers (Continued...1)
Lecture 21 - Stream Ciphers (Continued...2)
Lecture 22 - Pseudorandomness
Lecture 23 - Cryptographic Hash Functions
Lecture 24 - Cryptographic Hash Functions (Continued...1)
Lecture 25 - Cryptographic Hash Functions (Continued...2)
Lecture 26 - Message Authentication Codes
Lecture 27 - More Number Theoretic Results
Lecture 28 - The RSA Cryptosystem
Lecture 29 - Primality Testing

Get Digi-MAT (Digital Media Access Terminal) For High-Speed Video Streaming of NPTEL and Educational Video Courses in LAN

www.digimat.in

```
Lecture 30 - Factoring Algorithms
Lecture 31 - Some Comments on the Security of RSA
Lecture 32 - Discrete Logarithm Problem (DLP)
Lecture 33 - The Diffie-Hellman Problem and Security of ElGamal Systems
Lecture 34 - An Introduction to Elliptic Curve Cryptography
Lecture 35 - Application of Elliptic Curves to Cryptography
Lecture 36 - Implementation of Elliptic Curve Cryptography
Lecture 37 - Secret Sharing Schemes
Lecture 38 - A Tutorial on Network Protocols
Lecture 39 - System Security
Lecture 40 - Firewalls and Intrusion Detection Systems
Lecture 41 - Side Channel Analysis of Cryptographic Implementations
```

Get Digi-MAT (Digital Media Access Terminal) For High-Speed Video Streaming of NPTEL and Educational Video Courses in LAN

www.digimat.in