NPTEL Syllabus

Cryptography and Network Security - Video course

COURSE OUTLINE

The course deals with the underlying principles of cryptography and network security. It develops the mathematical tools required to understand the topic of cryptography.

Starting from the classical ciphers to modern day ciphers, the course provides an extensive coverage of the techniques and methods needed for the proper functioning of the ciphers.

The course deals with the construction and cryptanalysis of block ciphers, stream ciphers and hash functions.

The course defines one way functions and trap-door functions and presents the construction and cryptanalysis of public key ciphers, namely RSA.

The key exchange problem and solutions using the Diffie-Hellman algorithm are discussed. Message Authentication Codes (MAC) and signature schemes are also detailed.

The course deals with modern trends in asymmetric key cryptography, namely using Elliptic Curves. The course concludes with the design rationale of network protocols for key exchange and attacks on such protocols.

COURSE DETAIL

A video course shall consist of 40 or more lectures with 1 hour duration per lecture.

Module	Topics
Introduction and Mathematical Foundations	Introduction
	Overview on Modern Cryptography
	Number Theory
	Probability and Information Theory
Classical Cryptosystems	Classical Cryptosystems
	Cryptanalysis of Classical Cryptosystems

NP-TEL

NPTEL

http://nptel.iitm.ac.in

Computer Science and Engineering

Pre-requisites:

Discrete Structures, Algorithms.

Additional Reading:

1. Wenbo Mao, "Modern Cryptography, Theory & Practice", Pearson Education.
2. Hoffstein, Pipher, Silvermman, "An Introduction to Mathematical Cryptography", Springer.
3. J. Daemen, V. Rijmen, "The Design of Rijndael", Springer.
4. A. Joux,"Algorithmic Cryptanalysis", CRC Press.
5. S. G. Telang, "Number Theory", Tata Mc Graw Hill.
6. C. Boyd, A. Mathuria, "Protocols for Authentication and Key Establishment", Springer.
7. Matt Bishop, "Computer Security", Pearson Education.

Hyperlinks:

www.cse-web.iitkgp.ernet.in/~debdeep/courses_iitkgp/Crypto/index.htm

Coordinators:

Dr. Debdeep Mukhopadhyay
Department of Computer Science and EngineeringIIT Kharagpur

	Shannon’s Theory: I
	Shannon’s Theory: II
	Shannon’s Theory: III
Symmetric Key Ciphers	Symmetric Key Ciphers
	Modern Block Ciphers (DES)
	Modern Block Cipher (AES)
	Modern Block Cipher (AES) contd.
Cryptanalysis of Symmetric Key Ciphers	Linear Cryptanalysis
	Differential Cryptanalysis
	Other Cryptanalytic Techniques
	Overview on S-Box Design Principles
	Modes of operation of Block Ciphers
Stream Ciphers and Pseudorandomness	Stream Ciphers
	Pseudorandom functions
Hash Functions and MACs	Hash functions: The Merkle Damgard Construction
	Message Authentication Codes (MACs)
Asymmetric Key Ciphers: Construction and Cryptanalysis	More Number Theoretic Results
	The RSA Cryptosystem
	Primality Testing
	Factoring Algorithms

	Other attacks on RSA and Semantic Security of RSA
	The Discrete Logarithm Problem (DLP) and the Diffie Hellman Key Exchange algorithm
	The ElGamal Encryption Algorithm
	Cryptanalysis of DLP
Digital Signatures	Signature schemes: I
	Signature schemes: II
Modern Trends in Asymmetric Key Cryptography	Elliptic curve based cryptography: I
	Elliptic curve based cryptography: II
Network Security	Secret Sharing Schemes
	A Tutorial on Network Protocols, Kerberos
	Pretty Good Privacy (PGP)
	Secure Socket Layer (SSL)
	Intruders and Viruses
	Firewalls

References:

1. Douglas Stinson, "Cryptography Theory and Practice", 2nd Edition, Chapman & Hall/CRC.
2. B. A. Forouzan, "Cryptography & Network Security", Tata Mc Graw Hill.
3. W. Stallings, "Cryptography and Network Security", Pearson Education.