Computational Number Theory & Cryptography - Web course

COURSE OUTLINE

The emphasis of the course is on the application of the number theory in the design of cryptographic algorithms.

The course will start with the notion of time complexity and with several elementary number theoretic algorithms.

Putting them together we will see how we can design several cryptographic algorithms.

As a part of cryptanalysis we will study several attacks on these algorithms as well as their remedies.

We will also study recent developments in elliptic curve cryptography and the use digital signatures and its variations for authentication.

COURSE DETAIL

Sl.No.	Topics	No.of Hours
1	**Computational Complexity:** Input Size, Complexity Classes etc.	2
2	**GCD Computation:** Euclid's Algorithm, Extended Euclid's Algorithm.	3
3	**Modular Arithmetic:** Groups, Solving Modular Linear Equations. Chinese Remainder Theorem. Modular Exponentiation, Discrete Logarithm Problem.	8
4	**Key Exchange:** Diffie Hellman, ElGamal, Massey-Omura. Computation of Generators of Primes.	4
5	**Public Key Cryptosystem:** RSA, Different Attacks & Remedies.	6
6	**Primality Testing:** Pseudoprimality Testing, Quadratic Residues, Randomized Primality Test & Deterministic Polynomial Time Algorithm.	5
7	**Factorization:** Quadratic-Sieve Factoring Algorithm, Pollard-Rho Method.	2
8	**Elliptic Curve Cryptosystem:** Theory of Elliptic Curves, Elliptic Curve Encryption & Decryption	7

NP-TEL

NPTEL

http://nptel.iitm.ac.in

Computer Science and Engineering

Pre-requisites:

Discrete Mathematics and Algorithms.

Coordinators:

Dr. Pinaki Mitra
Department of Computer Science and EngineeringIIT Guwahati

	Algorithms, Security of Elliptic Curves Cryptography, Elliptic Curve Factorization.	
9	**Digital Signatures:** Authentication Protocols, Digital Signature Standards (DSS). Proxy Signatures.	3
Total		**40**

References:

1. Introduction to Algorithms: T. H. Cormen, C. E. Leiserson, R. Rivest and C. Stein Prentice Hall India, 2nd Edition, 2002.
2. A Course in Number Theory and Cryptography: Neal Koblitz, Springer-Verlag, New York Inc. May 2001.
3. Cryptography and Network security: Principles and Practice, William Stallings, Pearson Education, 2002.
4. Introduction to Cryptography with Coding Theory, Second Edition, W. Trappe and L. C. Washington, Pearson Education 2007.
5. Cryptography: Theory and Practice, Douglas R. Stinson, CRC Press.
6. Randomized Algorithms, R. Motwani and P. Raghavan, Cambridge University Press, 1995.