COL759 Cryptography & Computer Security

Course plan

Introduction to Cryptography, Classical Ciphers: Simple substitution, Vigenère cipher, Hill cipher, Playfair cypher and their analysis

Perfect Secrecy, one-time pad, limitations of perfect secrecy, computational security

Introduction to Number Theory: Divisibility and the Euclidean algorithm, Congruence, Fermat's Little Theorem, Euler phi-function, Euler's Theorem, Wilson's Theorem, Quadratic residues and reciprocity

One way Function, Introduction to Public Key cryptography, RSA public-key encryption, Rabin public-key encryption, ElGamal public-key encryption, Knapsack public-key encryption

Prime number generators, Legendre and Jacobi symbols, Probabilistic primality tests: Fermat's test, Solovay-Strassen test, Miller-Rabin test, Comparison: Fermat, Solovay-Strassen, and Miller-Rabin, strong primes, Computing Modular Inverses

Factoring of large composite numbers, Algorithms for Factoring: Pollard's p - 1 Method, Pollard's Rho Method, The Quadratic Sieve Algorithm.

Cyclic Groups and Generators, The Discrete Logarithm and Diffie-Hellman key exchange

Algorithms for Computing Discrete Logarithms: The Baby-Step/Giant-Step Algorithm, The Pohlig-Hellman Algorithm, The Index Calculus Method

Digital Signature Schemes - An Overview, RSA Signatures, Signatures from Collision-Resistant Hashing, The Digital Signature Algorithm (DSA), SHA

Introduction to Symmetric key cryptography, Finite Field, Pseudo randomness, pseudorandom generators, RC4 stream cipher, security of RC4, Polynomials over finite field, irreducible polynomial, primitive polynomial, Linear and nonlinear shift register sequences, Cryptanalysis of LFSR based cryptosystem

Block cipher: DES, AES

Zero Knowledge protocols

Elliptic Curve Cryptography: Introduction to Elliptic Curves, Elliptic Curve Cryptosystems, The elliptic curve factoring algorithm.

As time permits, we may also cover more advanced topics such as Learning with Error & Ring Learning with Error, Secret Sharing, Distributed Signatures.

Textbooks:

1. Computer Security and Cryptography by Alan G. Konheim, John Wiley & Sons, Inc.
2. Handbook of Applied Cryptography by Alfred J. Menezes, Paul C. van Oorschot, Scott A. Vanstone, CRC Press.
3. Introduction to Modern Cryptography by Jonathan Katz and Yehuda Lindell, CRC PRESS.
4. A Graduate Course in Applied Cryptography by D. Boneh and V. Shoup.
5. Cryptography: Theory and Practice by Douglas Stinson, CRC Press.