COL 759 Cryptography & Computer Security

Course Syllabus

Lecture 1-3:	Introduction to Cryptography, Perfect Secrecy, one time pad, limitations of perfect secrecy, computational security
Lecture 3-4:	Introduction and Classical Ciphers: Simple substitution, Vigenere cipher, Hill cipher, Playfair cypher and their analysis
Lecture 5-6:	Introduction to Number Theory: Divisibility and the Euclidean algorithm, Congruence, Fermat's Little Theorem, Euler phi-function, Wilson's Theorem, Quadratic residues and reciprocity
Lecture 7-9:	One way Function, Introduction to Public Key cryptography, RSA public-key encryption, Rabin public-key encryption, ElGamal public-key encryption, Knapsack public-key encryption
Lecture 10-12:	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
Lecture 13-15:	Factoring of large composite numbers, Algorithms for Factoring: Pollard's p - 1 Method, Pollard's Rho Method, The Quadratic Sieve Algorithm.
Lecture 16:	Cyclic Groups and Generators, The Discrete Logarithm and Diffie-Hellman key exchange
Lecture 17-19:	Algorithms for Computing Discrete Logarithms: The Baby-Step/Giant-Step Algorithm, The Pohlig-Hellman Algorithm, The Index Calculus Method
Lecture 20-21:	Digital Signature Schemes - An Overview, RSA Signatures, Signatures from Collision-Resistant Hashing, The Digital Signature Algorithm (DSA), SHA
Lecture 22-25	Introduction to Symmetric key cryptography, Finite Field, Pseudorandomness, pseudorandom generators, RC4 stream cipher, security of RC4,, Polynomials over finite field, irreducible polynomial, primitive polynomial, Linear and non linear shift register sequences, Cryptanalysis of LFSR based cryptosystem
Lecture 26	Block cipher: DES, AES
Lecture 27	Zero Knowledge protocols
Lecture 28	Elliptic Curve Cryptography: Introduction to Elliptic Curves, Elliptic Curve Cryptosystems, The elliptic curve factoring algorithm

Duration of a lecture: 1 hours and 30 minutes

Text Books:

1. *A Graduate Course in Applied Cryptography (*V 0.4, September 2017 *)* by D. Boneh and V. Shoup.

2. *Introduction to Modern Cryptography* (2nd edition) by J. Katz and Y. Lindell, CRC Press

Reference

1. *Handbook of Applied Cryptography* by Alfred J. Menezes, Paul C. van Oorschot, Scott A. Vanstone, CRC Press