CIS 5371 Practical Aspects of Modern Cryptography

Credits: 3 credits

Textbook, title, author, and year:
Handbook of Applied Cryptography, Menezes, Oorschot, Vanstone, Chapman & Hall/CRC, 1997.
ISBN: 0-8493-8523-7

Reference materials:
Cryptography Theory and Practice (3rd edition), Stinson, Chapman & Hall/CRC, 2006.
ISBN: 978-1-58488-508-5

Introduction to Modern Cryptography (2nd edition), Katz and Lindell, Chapman & Hall/CRC, 2015.
ISBN: 978-1-4665-7026-9

Specific Course Information

Catalog Description: Topics to be covered: (A) Mathematical background, algorithmic number theory, classical crypto, implementation aspects of private-key crypto, implementation aspects of public-key crypto, and (b) Advanced topics on crypto such as crypto primitives, rational crypto, secure multiparty computation, hash functions, digital signatures, and privacy-preserving protocols.

Prerequisites: Graduate Status Level or MAD2104 and COP3014.

Specific Goals for the Course: This course enables the students to review basic mathematical aspects of applied cryptography as well as fundamental concepts of cryptographic algorithms. Furthermore, it enables the students to utilize these techniques in computing systems through programming languages.

Brief List of Topics to be Covered:
Terminologies and Security Models, Modular Arithmetic and Integer Representations, Prime Numbers, GCD and LCM, Euclidean Algorithm and Extended Euclidean Alg., Congruence, Primitive Root, Discrete Log and RNG, Functions, Injection, Surjection and Bijection

From Classical to Modern Cryptography, Stream Ciphers, Software Implementation of Block Cipher: DES and AES, Implementation of RSA, ElGamal and Rabin Algorithms Using Large Integers, Randomized Algorithms: Las Vegas and Monte Carlo Algorithms, Probabilistic Public-Key Encryption: Blum-Goldwasser, Secret Sharing Schemes, Rational Cryptography, Secure Multiparty Computation, Cryptographic Hash Functions, Hash Functions Based on Block Ciphers, Hash Functions Based on Modular Arithmetic, Digital Signatures, Digital Signatures With Message Recovery, Privacy-Preserving Protocols, Sealed-Bid Auctions and Secure Mechanism Design.