CDA 5326 Cryptographic Engineering

Credits: 3 credits

Textbook, title, author, and year:
The course will not follow a particular text book

Reference materials:
Materials will be provided in an ongoing basis. The following references will be optional to follow:

- Cetin Kaya Koc (Editor): Cryptographic Engineering. 1st edition, Springer, 2009
- Paar, Pelzl: Understanding Cryptography: A Textbook for Students and Practitioners. 1st edition, Springer, 2009 Hankerson, Menezes and Vanstone, Guide to Elliptic Curve Cryptography (Ch. 2, 3, 5)
- Menezes, van Oorschot and Vanstone, Handbook of Applied Cryptography (Chapters 2 and 14) (Available free online)
- Articles from IEEE Transactions on Computers, CHES/ECC workshops proceedings

Specific course information.

Catalog description:
This course provides application perspective of cryptography and focuses on the computations, engineering, and secure implementations. This is a course for students interested in hardware and software design in industry and real-world security and cryptographic applications. The course is devoted to the state-of-the-art in cryptographic hardware/software and embedded systems. The students will learn about computational algorithms and architectures as well as about cryptanalysis of the cryptographic devices. The students will re/learn programming of cryptographic primitives on ASM, C, and hardware (using VHDL). Real world applications include implementations on cellphones, FPGA, and IoT devices with 8-bit/16-bit microcontrollers.

Prerequisites:

Discrete Mathematics (MAD 2104) or permission of the instructor

Specific goals for the course:

This is a cryptography engineering course. The students learn about embedding cryptographic algorithms and architectures into security products such as embedded devices. They will learn about implementations on hardware and software platforms including FPGAs and CPUs.

Brief list of topics to be covered:

Introduction to Computer Security and Cryptography
Mathematical background: Number theory, abstract algebra, Finite fields.
Finite Field, prime Field, modular arithmetic, quadratic fields and arithmetic.
Multiplication over finite fields: super-serial, bit-level, digit-level, bit-parallel architectures
Multiplication over finite field: Karatsuba, subquadratic multipliers, systolic array multipliers, hybrid-double multipliers.
Multiplicative inversion, Fermatt's little theorem, extended Euclidean Algorithm over prime and binary fields.
Exponentiation over finite field, trace and half trace function over finite fields, constant-time and non-constant- time implementations.

Public key cryptography, Diffie-Hellman key exchange, RSA, Elliptic curve cryptography (ECC).
Implementations of RSA and Diffie-Hellman over binary fields and prime fields.
Elliptic curves, generic curves, Montgomery curves, Edwards curves, Hassian and Huff curves.
Implementations of Elliptic Curve Cryptography over prime fields, Group law, group operations, point multiplication, coordinates systems.
Implementations of Elliptic Curve Cryptography over binary fields (polynomial basis and normal basis). Side-channel attacks analysis, secure implementations, and countermeasures.
Digital Signature algorithms (ECDSA, El Gamal) and implementations, Security-level and key size, performance analysis on hardware and software platforms
Introduction to quantum computation and post-quantum cryptography: Lattice based cryptography, isogeny-based cryptography, and other candidates. Students' project presentations