COT 5930 Cryptographic Engineering

Credits: 3 credits

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

Reference materials:

N/A

Specific course information

This course is open to all graduate and undergraduate students from CE, CS, EE, and Math. This course discusses implementation of cryptographic algorithms and architectures.

Catalog description:

N/A

Prerequisites:

NA

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 cryptographic computations and engineering on hardware and software platforms.
- Mathematical background: number theory, abstract algebra, Finite fields.
- Finite Field Arithmetic, prime fields, binary fields and extension fields.
- Side-Channel attack resistance computation over software and hardware platforms, power analysis attacks ad timing attacks.
- Public key cryptography: RSA and Elliptic curve cryptography
- Elliptic curve cryptography in hardware and software, group law, group operations, single and double point multiplication, coordinates systems, ECDH, ECDSA, and ECIES.
- Security-level, key size, and attack complexity.
- Introduction to standardized cryptography based on NIST and IEEE standards.
- Post-quantum cryptography and modern aspects for cryptographic computations/engineering.
- Low-power, low-energy, and high-performance computations and implementations on software and hardware