SEC534 - Cryptographic Engineering

Fall 2020

This is an advanced level course on cryptographic algorithms and architectures.

Catalogue Data: Basic concepts of symmetric key cryptography, basic concepts of asymmetric key cryptography, software implementation methods, hardware implementation methods, side-channel analysis, side-channel resistant implementations, tamper-proof cryptographic architectures.

Prerequisite: Basic hardware design concepts, basic knowledge of an HDL (Verilog or VHDL), basic knowledge of python and C languages.

Instructor: Erdinç Öztürk
FENS 1089, erdinco@sabanciuniv.edu

Zoom link for lectures:
https://sabanciuniv.zoom.us/j/97229520787?pwd=SWlZNXVxM0dxenQ0RTU5K3A4VzZiQT09

Schedule: Monday 14:40 – 16:30, Zoom
Wednesday 08:40 – 09:30, Zoom
TBA, Zoom (Office Hours)
Textbook: No Textbook. Material will be provided throughout the semester.
Extra Material: Alfred J. Menezes, Scott A. Vanstone, and Paul C. Van Oorschot. 1996. Handbook of Applied Cryptography (1st. ed.). CRC Press, Inc., USA. http://cacr.uwaterloo.ca/hac/
Exam Dates: TBD

Midterms and Final
- Exams will be held online.
- Students will have exactly 3 hours to finalize their exams. Late submission will not be accepted.
- For each question, students will have a limited time to answer. For example, first 30 minutes will be reserved only for question #1, second 30 minutes will be reserved for question #2, etc.
- Students can type their answers on any piece of paper, take pictures and send it.
- During grading, a few students may be randomly selected and be subjected to an oral exam. This oral exam will include questions about the exams. If any student fails to answer questions about their exam, they will receive 0 from that exam.

Tentative Outline

- Finite Field Operations:
  - Arithmetic in Prime Fields
  - Arithmetic in Binary Extension Fields
- Public Key Cryptography
  - Elliptic Curve Cryptography
  - RSA
- Symmetric Key Cryptography
  - DES
  - AES
- Side Channel Analysis
- True Random Number Generators

Tentative Grading

HW (Total 6)	30%
Midterm exam #1	15%
Midterm exam #2	15%
Final exam	30%
Term Project	10%