SEC534 - Cryptographic Engineering
Fall 2021

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/98348180682?pwd=NXN3eUx3QmxFcU03dW11bkFmZ3YrUT09

Schedule:
Monday : 12:40-13:30
Wednesday : 14:40-16:30
Office Hours : TBA

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/

Niels Ferguson, Bruce Schneier, Tadayoshi Kohno. Cryptography Engineering: Design Principles and Practical Applications.

Exam Dates:
TBD

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 4)	20%
Midterm exam #1	20%
Midterm exam #2	20%
Final exam	30%
Term Project	10%