# CS 411/507 - Cryptography

**Fall 2021**

This is a three-credit introductory course on the methods, algorithms, techniques, and tools of data security and cryptography. After studying the theoretical aspects of cryptographic algorithms and protocols, we show how these techniques can be integrated to solve particular data and communication security problems. This course material is of use to computer and communication engineers who are interested in embedding security into an information system, and thus, providing integrity, confidentiality, and authenticity of the documents and the communicating parties.

**Catalogue Data:** Classical Cryptosystems, Basic Number Theory, Block Cipher Algorithms: DES, 3DES, and AES(Rijndael), Public Key Cryptography: RSA Discrete Logarithms, Elliptic Curve Cryptography (ECC), Digital Signatures, Implementation Issues, Secret Sharing, Zero Knowledge Techniques, Games, Digital Cash, Quantum Cryptography.

**Prerequisite:** The course is open to graduate and undergraduate students. Some experience in Python programming language is required.

**Instructor:** Erkay Savaş

 FENS 2037, x9501, erkays@sabanciuniv.edu

**Schedule:** Wednesday 17:40 - 19:30 (Lecture)

 Thursday 08:40 - 09:30 (Lecture)

 Wednesday 08:40 - 10:30 (Office Hours – Erkay Savaş)

 Tuesday 09:40 - 11:30 (Office Hours – Şeyma Selca Mağara)

 Wednesday 15:40 - 17:30 (Office Hours – Atıl Utku Ay)

Friday 10:40 - 12:30 (Office Hours – Anes Abdennebi)

**Textbook:** Nigel P. Smart. Cryptography Made Simple. Springer, 2016. ISBN 978-3-319-21936-3

**Reference:** W. Trappe and Lawrence C. Washington, Introduction to Cryptography with Coding Theory. 2nd Edition , Prentice Hall, 2006.

C. Paar and J. Pelzl, Understanding Cryptography, Springer 2010

A. J. Menezes P. C. van Oorschot, and S. A Vanstone. Handbook of Applied Cryptography, CRC

Press, 1997.

D. R. Stinson, Cryptography: Theory and Practice, 3rd Edition, Chapman & Hall/CRC, 2006.

## Tentative Outline

* **Introduction and Classical Cryptosystems:** Secure communication. Attacks to cryptosystems. Classical cryptographic techniques and algorithms. One-time pad, randomness and pseudo-randomness
* **Mathematical Foundations:** Number theory. Finite fields. Primitive roots. Exponentiation and discrete logarithm.
* **Secret-Key Cryptography:** Block ciphers and stream ciphers. DES, AES (Rijndael). Modes of operation.
* **Public-Key Cryptography:** One-way functions. Trapdoor one-way functions. Public-key cryptosystems. RSA, Diffie-Hellman, ElGamal, and elliptic curve cryptosystems.
* **Authentication and Digital Signatures:** Hash functions and message-digest functions. Digital signatures. Authentication protocols, forward secrecy, plausible deniability.
* **Protocols:** Zero-knowledge proof systems. Key management architectures, Public Key Infrastructure.

## Student Responsibilities (tentative)

* **Quizzes:** Therewill be about 10 quizzes that may be held outside of lecture hours. No makeup exam will be offered if you miss one for any reason.
* **Exams:** Students are required to comply with instructor’s rules for exams (quizzes, midterm, and final)
* **Homework assignments:** There will be about four homework assignments. You will be required to write programs in Python programming language.
* **Term project:** Students are required to work on a term project. It is essential for students to meet time schedule of the projects. Project groups must provide a demonstration/presentation of their work. During the demonstration/presentation, all the project members must be present. Students may work in groups of two.

## Grading (tentative)

Midterm exam (Physical) 30%

Final exam (Physical) 35%

Quiz 10%

Homework 10%
Project 15%

## Class Website: http:// people.sabanciuniv.edu /~erkays/cs411\_507