CS 411/507 - Cryptography
Fall 2022 - 2023

Instructor Information

Name:	Atıl Utku Ay
Office:	FENS L026
Email:	utku.ay@sabanciuniv.edu
Office Hours:	TBA

Schedule

Lectures:	Wednesday	15:40 - 16:30	FENS G077
	Thursday	08:40 - 10:30	UC G030

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 class is open to any undergraduate students, who have previously taken MATH 204 – Discrete Mathematics - and scored minimum grade of D. Additionally, some experience in Python programming language is required.

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.

Textbook

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

References

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.

Student Responsibilities

- **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.

Tentative Grading

- Midterm Exam 30%
- Final Exam 40 %
- Term Project 15%
- Homeworks (Total 4($\pm$1)) 15%

In order to pass the course, the Final Exam and the overall grades of the students must be at least 25/100 and 35/100, respectively. The other letter grade boundaries will be determined by the instructor at the end of the term.

Exams will be held in-person.

Exam Dates

Midterm:	TBA (possibly 8^{th} or 9^{th} week of the term)
Final:	will be scheduled by SR

Make-up Policy

- There will be no make-up for homeworks, labs, and term project. Students automatically get 0 (zero) from the respective assignment grade if any of them is missed.
- Make-up is only allowed for the midterm and final examinations to those with an official medical report and to those with an official permission notice from the university on the date of the exam in question.
- Make-up examinations may be written and/or oral.

Plagiarism Policy (Academic Integrity)

Plagiarism means presenting someone else's work as yours. This is a very serious and ethical problem. A plagiarized work may or may not be a verbatim copy of another submission. Verbatim copies are of course plagiarized ones. However, if a submission is derived from another one by partially changing some parts, this action is also plagiarism. When a plagiarism case is detected, sanctions are applied to all parties regardless of the actual source of the submission. These sanctions are as follows:

- For the midterm/final examinations,
  - students directly fail the course, even in the first offense.[1]
- For the homeworks and term project,
  - for the first time, all plagiarized submission owners receive -100,
  - the second time, the student fails the course automatically. [2]

[1] Additionally, the case will be referred to the FENS Dean's Office for disciplinary action. This course does not tolerate any breach of academic integrity (more info on https://www.sabanciuniv.edu/en/academic-integrity-statement)

[2] See footnote 1