COMP 430/530: Data Privacy and Security

Koç University, Fall 2024

Course Description

This course will cover major developments in statistical data privacy and security in the past two decades, fundamentals of state-of-the-art privacy methods used in the digital world, as well as recent research trends in privacy and security. The course is intended to: (i) provide students with breadth in the areas of data privacy and security through lectures and homework assignments; and (ii) enable students to specialize in a privacy-related or security-related topic of their own choice through a course project. The course is suitable for graduate students and accomplished undergraduates who are interested in privacy and security.

Instructor: M. Emre Gürsoy – www.memregursoy.com – emregursoy@ku.edu.tr

KU Credits: 3

Meeting Times & Location: TBA

PS/DS/Lab: No

Language of Instruction: English

Office Hours: Time TBA, location my office (SNA Z27). TAs will also hold office hours. All office hour information will be announced after the semester begins.

Teaching Assistants (TAs): TBA

Prerequisites: COMP 202 (Data Structures and Algorithms) for undergraduates. No formal prerequisites for graduates, but equivalent knowledge is expected.

Recommended Background: Although the following are not official prerequisites for the course, based on past experience, I strongly recommend students to have:

- Maturity in computer science concepts, discrete math, databases, and statistics. Having done well in *COMP 106 (Discrete Mathematics for Computer Science and Engineering)* and *ENGR 200 (Probability and Random Variables for Engineers)*, or their equivalent, will increase your chances of being successful in this course.
- Programming experience, especially in Python. The course does not involve heavy programming, but you should be proficient in Python (or be willing to learn quickly).

List of Topics

- Introduction and preliminaries
- Data anonymization (k-anonymity, l-diversity, t-closeness)
- Differential privacy
- Local differential privacy
- Machine learning for security

- Security for machine learning (adversarial machine learning, training-time and test-time attacks, introduction to privacy-preserving machine learning)
- Authentication mechanisms (passwords, threats to passwords and authentication mechanisms, dictionary attacks, salting)
- Database security (access control, SQL injection)
- [tentative] Principles of modern privacy laws and regulations, e.g., GDPR, KVKK

Grading (Tentative)

Midterm Exams	–	50%
Course Project	–	25%
Homework Assignments	–	22%
Peer Reflections	–	3%

Based on the circumstances, these percentages are subject to change (at most 5%) at the instructor's discretion.

Midterm Exams: We will have two midterm exams, each worth 25%, total 50%. The average of your two midterms must be **at least 30** to pass the course.

Homework Assignments: There will be 4 homework assignments, totaling 22% of the course grade. They will be announced and collected via Blackboard. Majority of the problems in the homework assignments will be programming problems, but there may also be some math problems, proofs, and verbal questions. For programming problems, Python will be the primary programming language. HWs can have different weights (e.g., HW1 is more difficult, so it will likely have a higher weight than other HWs). **All HWs must be completed individually; collaboration is not allowed.**

Course Project: The course project enables students to specialize in a privacy or security-related topic of their own choice. We are looking for **research**-style course projects, i.e., your project should go beyond what is taught in class, and contain some novelty in terms of idea, design, development, and/or experimentation. Students are encouraged to pick a project topic that relates to their personal expertise and interests. The instructor will also suggest sample project topics. Students are encouraged to discuss one-on-one with the instructor to define a suitable and exciting project. Course projects will be due in the finals week.

Course projects can be done in groups. A minimum and maximum group size limit will be enforced depending on how many students are taking the course, e.g.: min 1 student, max 4-5 students per group.

The grade for the course project (25%) is divided into multiple items:

- Project proposal (5%)
- In-class project presentation (5%)
- Final project report and deliverables (15%)

The course project is meant to be innovative and enjoyable for you. It is intentionally left open-ended to give you experience in working on a small research project, e.g., searching for relevant publications and resources, reading and learning by yourself, and defining and solving a research problem. Promising projects may be extended to future semesters for research credits (e.g., Independent Study), publications, etc. Talk to me if you are interested.

Peer Reflections: In the last weeks of the semester, each group will give a short presentation (e.g.: 10-15 minutes) of their project during lecture hours. Students are expected to attend other groups' presentations and write peer reflections. Each peer reflection should be approximately half-page long and consist of the following parts:

- Summary: 4-5 sentences to summarize the presentation/project
- Strengths: 2-3 bullet points to list the main strengths and advantages of the project
- Weaknesses: 2-3 bullet points to list the main weaknesses, shortcomings, and potential improvements for future work

Homework Policies

For late submission of homework assignments, we have the following policy:

- Up to 10 minutes late: -5% penalty
- 10 minutes to 1 hour late: -20% penalty
- More than 1 hour late: submission is not accepted

Assignments submitted more than 1 hour after the deadline will not be accepted unless the instructor's permission is obtained ahead of time with a valid excuse. Please do not ask for an extension close to a deadline or after a deadline that has passed. In order to be fair to students who submitted the assignment on time, such requests are almost always rejected.

In general, it is the student's responsibility to ensure that his/her homework submission is complete and includes all the files that the student was intending to submit. For hand-written submissions, it is again the student's responsibility to make sure that his/her handwriting is legible, and the scan/photo has sufficient quality so that the homework can be graded.

[*IMPORTANT, READ ME*] Exam Policy

As of the beginning of the semester, all exams are planned to be conducted physically, in-person. Unless there is a university-wide rule that enforces online exams for all courses and all students, I will not offer an online exam to any individual student. There will be no exceptions to this rule. All students who are taking this course are assumed to have read and understood this rule.

Make-Up Policy

If a student misses a midterm or final exam with a valid excuse, he/she can apply for a make-up. For excuses to be valid, they must be accepted by Koç University and communicated with the instructor through official channels. Emergencies must be properly documented, and medical reports must be approved by Koç University Health Center. Do not send health reports directly to the instructor.

A single, joint make-up exam will be given at the end of the semester, which will cover all topics in the course. Regardless of which exam they missed, all students who are eligible for a make-up will take this exam. The grade they receive from the make-up will count in place of the exam they originally missed.

Academic Honesty Policy

Students may only collaborate on the course project. Remaining parts of the course must be completed individually. Violation of this rule constitutes academic dishonesty.

Academic dishonesty is a serious violation of the trust upon which an academic community depends. By taking this course, students acknowledge that they must fully comply with Koç University's Student Code of Conduct (https://apdd.ku.edu.tr/en/academic-policies/student-code-of-conduct/). Violations of the Student Code of Conduct, including cheating and plagiarism, will be reported to the University Disciplinary Committee.

Cheating will not be tolerated! Cheating includes but is not limited to: working jointly with another student on an assignment/exam, sharing your assignment answers with others, looking at another student's assignment/exam, having someone else do an assignment/exam for you (paid or not), taking screenshots of homework and exam questions, distributing homework and exam questions and answers to others.

Use of Generative AI

In general, all work that you submit must be based on **your** knowledge and ideas, and you must take full responsibility for them. Thus, it is forbidden to use a generative AI tool (such as ChatGPT) to do your homework or project on your behalf. When checking for plagiarism, we will also compare your submissions against solutions we obtain from generative AI.

On the other hand, it is acceptable to use AI tools to polish your writing. For example, consider that you are writing your project proposal or final report. First, you should write your draft based on your own knowledge and ideas. Afterward, it is OK to use AI tools to fix errors, improve your writing and clarity, etc. But the main substance of your work and its technical merits should come from you, not an AI tool.

Attendance and Recording Policy

This policy is subject to change according to announcements made by YÖK and/or Koç University.

- Lectures will be held from the assigned classroom. In most lectures, slides and whiteboard will be used simultaneously.
- Lecture recordings will be shared via Panopto. I highly recommend not relying on Panopto recordings alone. Instead, attend the lectures. Experience from previous semesters shows that there is a strong correlation between regular lecture attendance and letter grades.
- Although there is no penalty for not attending lectures, I take attendance several times during the semester (unannounced) and give a few bonus points at the end of the semester based on lecture attendance.