PRIVACY ENHANCING TECHNOLOGIES (PETS)
EECS 598-XXX WINTER 2023
INSTRUCTOR: TODD M. AUSTIN

Overview: This course explores the latest advances in privacy-enhancing technologies (PETs). The privacy technology field is an exciting research arena with significant promise to ease the tension between data privacy and data discovery. For example, using modern PETs it is now possible to analyze human genomes without researchers having the ability to see those genomes. Similarly, enterprises can use PETs to share statistics about their users with strong guarantees that those statistics do not reveal any information about a single user. In this course, we will explore privacy technology research, with focus on tools, technologies, and applications. Upon completing the course, students should feel well prepared to take on the privacy-oriented programming and data analysis challenges that they will undoubtedly encounter.

Course Prerequisites: The course requires graduate standing in CSE. It is assumed that students have prior programming and data science experience. No previous experience with computer security or privacy technologies is necessary.

Course Structure: The course will include lectures, a late mid-term exam, and a semester-long team-based privacy-oriented research project. Lectures will be given by a combination of instructor lectures, visiting lecturers, and student presentations. The reading material for the course will be from recent and classic published papers from privacy-related conferences.

Course Syllabus: The course will first motivate the need for privacy-enhancing technologies, then focus on how they are used in real-world applications, followed by a tour of the primary technologies available today to those wanting to improve their privacy practices.

- Why privacy matters
  - Privacy vs. security
  - Privacy risks
- Privacy technology use cases
  - Improving consumer trust
  - Data discovery without privacy risks
  - Overcoming regulatory barriers
- Statistical privacy techniques
  - Differential privacy
  - Differentially private machine learning
  - Federated machine learning
- Anonymization techniques
  - Tokenization
  - Synthetic data
- Secure computation
  - Secure multi-party computation
  - Homomorphic encryption
  - Trusted Execution Environments
  - Zero-knowledge proofs
  - Functional encryption
  - Sequestered encryption

Course Instructor: Prof. Todd Austin <austin@umich.edu>