TO: The Faculty of the College of Engineering

FROM: Elmore Family School of Electrical and Computer Engineering

RE: New Graduate Course, ECE 50877 Introduction to Applied Cryptography

The faculty of the School of Electrical and Computer Engineering has approved the following new course. This action is now submitted to the Engineering Faculty with a recommendation for approval.

ECE 50877 Introduction to Applied Cryptography
Sem. 1, Lecture 3, Cr. 3.
Prerequisite: graduate student standing

Description: Cryptography is an essential component of securing communication and data in a wide range of applications. This course explores fundamental building blocks in cryptography such as ci-phers, hash functions, and digital signatures. We will then demonstrate how these building blocks are used practically to secure communications and systems. We will also learn about the power of advanced cryptog-raphy to enable complex functionalities with rigorous security guarantees. We will cover fundamental secure multiparty computation protocols and review their application in building secure and privacy-preserving systems. We will also explore social and ethical issues in developing and deploying cryptographic systems.

Reason:
This course fills a void in the department for graduate students who do security research or are interested in computer security in general.

Course History: Fall 2023 – 11, Fall 2024 – 20

Mithuna Thottethodi,
Associate Head for Teaching and Learning
Elmore Family School of Electrical and Computer Engineering

Introduction to Applied Cryptography

Tentative course outline:

Week	Lecture
01	Introduction and historical ciphers
02	Computational security, pseudorandom number generators, symmetric encryption
03	Message authentication, security definitions
04	Hash functions and practical constructions
05	Number theory and hardness assumptions
06	Public key cryptography
07	Digital signatures, certificates, public key infrastructure
08	Identity verification and code signing
09	GPG, web of trust, SSL/TLS
10	Secret sharing and threshold cryptosystems
11	Oblivious transfer and Yao's garbled circuits
12	Partial homomorphic encryption and commitment schemes
13	Cryptography in emerging technologies (AI and IoT)
14	Ethics of cryptographic work
15	Last week of class – project presentations