THE OHIO STATE UNIVERSITY

COLLEGE OF ENGINEERING

Introduction to Cryptography

CSE 5351

Credit Hours:
3.00

Course Levels:
Undergraduate (1000-5000 level)
Graduate (5000-8000 level)

Course Components:
Lecture

Course Description:
Foundations of cryptography; mathematical formulations/proofs of security goals; theory and practical constructions of encryption schemes, MACs, digital signatures; zero-knowledge proof systems; cryptographic protocols.

Prerequisites and Co-requisites:
Prereq: 2331 (680), 5331, Math 4573 (573), or 4580 (580), and Stat 3460 (427) or 3470.

Course Goals / Objectives:

- Master various symmetric-key and public-key encryption schemes
- Be competent with basic cryptographic protocols such as key exchange, identification, and commitment schemes
- Be familiar with cryptographic hash functions, message authentication codes, and digital signatures
- Be familiar with mathematical foundations of cryptography and mathematical formulations of security goals
- Be exposed to zero-knowledge proof systems
- Be exposed to advanced cryptographic protocols such as electronic voting and digital cash
- Be exposed to cryptographic attacks

Course Topics:

- Mathematical background
- Foundations of cryptography: computational indistinguishability, one-way functions/permutations, hard-core predicates, pseudorandom generators, pseudorandom functions/permutations.
- Mathematical formulations of security goals: ciphertext indistinguishability against eavesdroppers, chosen-plaintext attackers, chosen-ciphertext attackers.
- Symmetric-key encryption: encryption schemes based on pseudorandom generators/functions/permutations, practical encryption schemes such as DES and AES.
- Public-key encryption: trapdoor one-way functions/permutations, RSA, attacks on RSA, padded-RSA, optimal asymmetric encryption padding (OAEP), random oracles, security against chosen-plaintext and chosen-ciphertext attacks, ElGamal encryption scheme.
- Hash functions, message authentication codes, digital signatures
- Zero-knowledge proof systems, commitment schemes, identification schemes.
- Cryptographic protocols such as key exchange, entity authentication, watermarking, electronic voting, digital cash.

Designation:
Elective