CSE 5351 (Approved): Introduction to Cryptography

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.

Prior Course Number: CSE 723
Transcript Abbreviation: Intr Cryptography
Grading Plan: Letter Grade
Course Deliveries: Classroom
Course Levels: Undergrad, Graduate
Student Ranks: Senior, Masters, Doctoral
Course Offerings: Spring
Flex Scheduled Course: Never
Course Frequency: Every Year
Course Length: 14 Week
Credits: 3.0
Repeatable: No
Time Distribution: 3.0 hr Lec
Expected out-of-class hours per week: 6.0
Graded Component: Lecture
Credit by Examination: No
Admission Condition: No
Off Campus: Never
Campus Locations: Columbus
Prerequisites and Co-requisites: (Stat 3460 or Stat 3470 or Stat 427) and (CSE 2331 or CSE 5331 or CSE 680 or Math 4573 or Math 573 or Math 4580 or Math 580)
Exclusions: Not open to students with credit for CSE 723 or CSE 794Q
Cross-Listings:

The course is required for this unit's degrees, majors, and/or minors: No
The course is a GEC: No
The course is an elective (for this or other units) or is a service course for other units: Yes

Subject/CIP Code: 14.0901
Subsidy Level: Doctoral Course

Programs

Abbreviation	Description
BS CSE	BS Computer Science and Engineering
MS CSE	MS Computer Science and Engineering
PhD CSE	PhD Computer Science and Engineering

General Information

Students are expected to be comfortable with mathematical reasoning.

Course Goals

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

Topic	Lec	Rec	Lab	Cli	IS	Sem	FE	Wor
Mathematical background	3.0							
Foundations of cryptography: computational indistinguishability, one-way functions/permutations, hard-core predicates, pseudorandom generators, pseudorandom functions/permutations.	3.0							
Mathematical formulations of security goals: ciphertext indistinguishability against eavesdroppers, chosen-plaintext attackers, chosen-ciphertext attackers.	3.0							
Symmetric-key encryption: encryption schemes based on pseudorandom generators/functions/permutations, practical encryption schemes such as DES and AES.	6.0							
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.	6.0							
Hash functions, message authentication codes, digital signatures	6.0							
Zero-knowledge proof systems, commitment schemes, identification schemes.	6.0							
Cryptographic protocols such as key exchange, entity authentication, watermarking, electronic voting, digital cash.	6.0							

Grades

Aspect	Percent
Homework	20%
Midterms	50%
Final	30%

Representative Textbooks and Other Course Materials

Title	Author
Introduction to Modern Cryptography	Jonathan Katz & Yehuda Lindell
Introduction to Cryptography: Principles and Applications (2nd edition)	Hans Delfs & Helmut Knebl

ABET-EAC Criterion 3 Outcomes

Course Contribution		College Outcome
***	a	An ability to apply knowledge of mathematics, science, and engineering.
	b	An ability to design and conduct experiments, as well as to analyze and interpret data.
**	c	An ability to design a system, component, or process to meet desired needs.
	d	An ability to function on multi-disciplinary teams.
**	e	An ability to identify, formulate, and solve engineering problems.
*	f	An understanding of professional and ethical responsibility.
	g	An ability to communicate effectively.
**	h	The broad education necessary to understand the impact of engineering solutions in a global and societal context.
*	i	A recognition of the need for, and an ability to engage in life-long learning.
***	j	A knowledge of contemporary issues.
***	k	An ability to use the techniques, skills, and modern engineering tools necessary for engineering practice.

BS CSE Program Outcomes

Course Contribution		Program Outcome
***	a	an ability to apply knowledge of computing, mathematics including discrete mathematics as well as probability and statistics, science, and engineering;
	b	an ability to design and conduct experiments, as well as to analyze and interpret data;
	c	an ability to design, implement, and evaluate a software or a software/hardware system, component, or process to meet desired needs within realistic constraints such as memory, runtime efficiency, as well as appropriate constraints related to economic, environmental, social, political, ethical, health and safety, manufacturability, and sustainability considerations;
	d	an ability to function on multi-disciplinary teams;
***	e	an ability to identify, formulate, and solve engineering problems;
*	f	an understanding of professional, ethical, legal, security and social issues and responsibilities;
	g	an ability to communicate effectively with a range of audiences;
	h	an ability to analyze the local and global impact of computing on individuals, organizations, and society;
*	i	a recognition of the need for, and an ability to engage in life-long learning and continuing professional development;
***	j	a knowledge of contemporary issues;
**	k	an ability to use the techniques, skills, and modern engineering tools necessary for practice as a CSE professional;
***	l	an ability to analyze a problem, and identify and define the computing requirements appropriate to its solution;
***	m	an ability to apply mathematical foundations, algorithmic principles, and computer science theory in the modeling and design of computer-based systems in a way that demonstrates comprehension of the tradeoffs involved in design choices;
	n	an ability to apply design and development principles in the construction of software systems of varying complexity.

Prepared by: Ten-Hwang Lai