Foundations of Cryptography - CS/CPE 579

Syllabus

Stevens Institute of Technology

Spring 2024

Instructor Prof. Nikos Triandopoulos

Contact Info: ntriando@stevens.edu, (201) 216-3751

Office Hours: Tuesday, 2:00 - 3:00pm, GS 428, or by appointment

Teaching Assistant Staff

Devharsh Trivedi, 5th year PhD student, dtrived5@stevens.edu

Course Information

Canvas Course Address: 2024S CS/CPE 579-A
Course Format: On campus
Course Schedule: CS 579, Tuesday, 3:30pm - 6:00pm, GS 216
Course Prerequisite: CS503 and (CS385 or CS570 or CS590) and (Grad Student/Junior/Senior)

Course Description

Per Academic Catalog
This course provides a broad introduction to cornerstones of security (authenticity, confidentiality, message integrity, and non-repudiation) and the mechanisms to achieve them as well as the underlying mathematical basics. Topics include block and stream ciphers, public-key systems, key management, certificates, public-key infrastructure (PKI), digital signatures, non-repudiation, and message authentication. Various security standards and protocols such as DES, AES, PGP, and Kerberos, are studied.

Per Instructor
The course provides a broad introduction to the cornerstones of security by studying core properties, such as authenticity and confidentiality, through the lens of modern cryptography, thus emphasizing rigorous design and analysis frameworks via careful use of the underlying mathematical principles, but also with a focus on real-world cryptography, thus paying attention to practical design and implementation considerations for effectively and efficiently securing computer systems across broad application areas in today's era of outsourced computing.

Learning Objectives

After successful completion of this course, students will be able to:

1. Discuss how cryptography helps to achieve common **security goals** and tasks.
2. Explain the notions of **core cryptographic primitives**, both **symmetric**, such as symmetric encryption, hash functions and message authentication codes, and **asymmetric**, such as public-key encryption and digital signatures.
3. Sketch **formal security definitions** and describe prominent **implementation techniques** for such primitives.
4. Illustrate the difference between **symmetric Vs. asymmetric** cryptography.
5. Evaluate cryptographic primitives & their implementations for **correctness**, **efficiency** and, importantly, **security**.

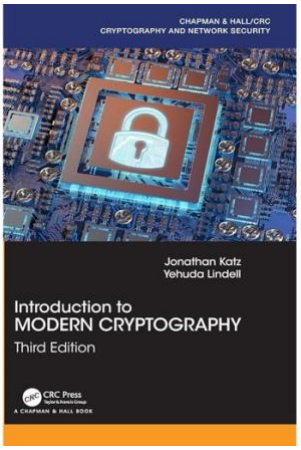
Course Structure

Weekly lectures, homework assignments, paper-analysis assignments, and a final project, but no midterm or final exam.

Course Materials

1. Lecture notes – provided in the classroom as presentation slides or on the whiteboard;
2. Practice quizzes, solutions to assignments or external reading resources – provided on Canvas;
3. Required textbook:

Introduction to Modern Cryptography,
by J. Katz & Y. Lindell;
3rd edition, CRC Press, Chapman & Hall;
Offered as e-book or hardcopy.



Course Requirements

- **Attendance**
  - Students are generally required to attend lectures.

- **Participation**
  - Students are required and strongly encouraged to participate in the classroom, by asking questions, answering questions asked by the instructor, and leading or participating in discussions help in coordination with the instructor.
- **Assignments**
  - Students are required to hand in their individual homework solutions by the specified deadline.
- **Final Project**
  - Students are required to work (individually or in small groups) on a final project.
  - Specific instructions and guidelines related to final projects are provided below and will also be covered in detail in the class.

Final Projects

There will be no midterm or final exams in this course. Instead, students will have to work, individually or in teams (of small size, e.g., in groups of 2-3 students) on a final project. Final projects will take the form of handing in a report and giving a short presentation to the entire class in a predetermined date close to or during the final examination period. Project types and specific topics are to be decided by each student or team in coordination with the instructor. Possible project types include, but are not limited to, survey papers on cryptographic technologies, implementation of specific security tools, analysis of real-world cyber-attacks, or presentation of special topics of interest that relate to the course contents. More information about the logistics (e.g., team formation, suggested topics, exact format, general timeline, involved deadlines, etc.) will be provided in class at the beginning of the course.

Late Assignment Policy

Each homework assignment has a deadline, typically two weeks after the time the assignment is posted, by which date solutions musts be handed in.

Late submissions are accepted but subject to the following rules:

- Each student has three (3) free "late" days which can be used when needed (or at the student's discretion) for late submissions.
- Each "late" day will be used automatically and as a whole – for example, if the deadline of the first assignment is at midnight and a student submits their answers at 7am of the following morning, then one of the student's three free "late" days is necessarily used.
- After three "late" days have been used, the following late-submission policy comes in effect: Each extra used "late" day (defined as above) incurs a 10% reduction to the grade of the assignment – for example, a perfect solution to the first assignment submitted 4 days and 1 hour after the deadline is graded with 80/100 (instead of 100/100).

Course Requirements & Grading

Students will be evaluated based on class attendance and participation, homework assignments and the final project. Grades will be tentatively calculated using the following weights:

Class Attendance & Participation	(20%)
Assignments	(40%)
Final Project	(40%)

Tentative Course Schedule

Week	Topic	Readings	Assignment
	Introduction		
1, 1/23	Course logistics, symmetric-key encryption, historical ciphers, and principles of modern cryptography	Sections 1.1 - 1.4 & related lecture notes	-
	Perfect Secrecy		
2, 1/30	Information-theoretic ciphers, the One-Time Pad encryption, and its security & efficiency analysis	Sections 2.1 - 2.3 & related lecture notes	-
	Symmetric Encryption		
3, 2/06	Computational security, negligible functions, basic EAV-secure encryption, multiple encryptions, chosen-plaintext attacks (CPAs), and CPA-security	Sections 3.1 - 3.2, 3.4 & related lecture notes	HW1
	Pseudorandomness		
4, 2/13	Pseudorandom generators (PRGs), pseudorandom functions (PRFs), and their implementation in practice as stream ciphers and block ciphers	Sections 3.3.1, 3.5.1, 7.1 - 7.2 & related lecture notes	-
	Provable Security		
5, 2/20	Proofs by reduction, EAV- and CPA-secure fixed-length ciphers, their security proofs, and domain extension via modes of operations	Sections 3.3, 3.5 - 3.6 & related lecture notes	HW2

	Message Authentication		
6, 2/27	Message integrity, message authentication codes (MACs), and generic constructions (fixed-length, domain extension, CBC-MAC)	Sections 4.1 - 4.4 & related lecture notes	-
	Hash Functions		
7, 3/05	Cryptographic hash functions, domain extension via the Merkle-Damgård framework, applications to MAC design ('hash & MAC', HMAC), the SHA2 class of cryptographic hash functions, birthday attacks, and the random oracle model	Sections 6.1 - 6.5, 7.3 & related lecture notes	HW3
3/12	*No Class (Spring Break)*		-
	Practical Applications		
8, 3/19	Authenticated encryption (chosen-plaintext attacks (CCAs), CCA-security, secure communication sessions), and hash-based security solutions (fingerprinting, deduplication, Merkle trees, digital envelops)	Sections 5.1 - 5.4, 6.6 & related lecture notes	Project Ideas
	Asymmetric Cryptography		
9, 3/26	Key management, motivation for public-key (PK) cryptosystems, the concepts of PK encryption & digital signatures, digital certificates, and hybrid encryption	Sections 11.1 - 11.2, 11.4, 12.1 - 12.3, 13.1 - 13.3, 13.6 & related lecture notes	HW4

	Discrete-log based schemes		
10, 4/02	Number theory basics, discrete logarithm & Diffie-Hellman (DH) assumptions, DH-based key agreement, El Gamal encryption, and El Gamal digital signatures	Sections 9.1, 9.3, 11.3, 12.4, 13.5 & related lecture notes	-
	RSA based schemes		
11, 4/09	Factoring & RSA assumptions, and the RSA cryptosystem (RSA algorithm, plain RSA, padded RSA, PKCS extensions)	Sections 9.2, 12.5, 13.4 & related lecture notes	Project Preparation
12, 4/16	**Special Topics I** Post-quantum cryptography	TBD	-
13, 4/23	**Special Topics II** Secret sharing & applications	TBD	-
15, 4/30	***Project Presentations***		Final Project
Exam Period	***Project Presentations***		Final Project

Academic Integrity

This is a 500-level course, thus governed by the following three academic integrity policies:

- Graduate students in CS579/CPE579 are bound by the **Graduate Student Code of Academic Integrity**.
- Undergraduate students in CS579/CPE579 are bound to the **Special Provisions for Undergraduate Students in 500-level Courses.** That is, undergraduate students are bound to the **Undergraduate Honor System but not fully, according to special provisions** that have been agreed upon by the Dean of Graduate Academics and the Honor Board.