

Syllabus

Logo.jpg

Foundations of Cryptography - CS/CPE579-A

Stevens Institute of Technology

Spring 2023

cybersecurity2.jpg

Instructor Prof. Nikos Triandopoulos

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

Office Hours:

Tuesday, 2:00 - 3:00pm, Gateway South Building 428, or by appointment, or via Zoom (remotely, as needed)


Teaching Assistant Staff

Devharsh Trivedi, 4th year PhD student, dtrived5@stevens.edu
(<mailto:dtrived5@stevens.edu>)

Course Information

Canvas Course Address: 2022S CS 579-A

Course Format: On campus, or Online (distance learning, as needed)

To access the course when offered online, please visit stevens.edu/canvas  (<http://stevens.edu/canvas>). For more information about course access or support, contact the TRAC by calling 201-380-6599 or 201-216-5500.

Course Schedule:

CS579-A, Tuesday, 3:30pm - 6:00pm, Burchard 111, or via Zoom (remotely, as needed)

Course Prereqs:

- CS503 or MA503 and CS385 or CS182, or
- CS503 or MA503 and CS570 or CS590

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 signature, 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 principles via careful use of the underlying mathematical basics, but also with a focus on **real-world cryptography**, thus paying attention to practical implementation mechanisms for securing existing application areas in the era of outsourced computing.

Learning Objectives

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

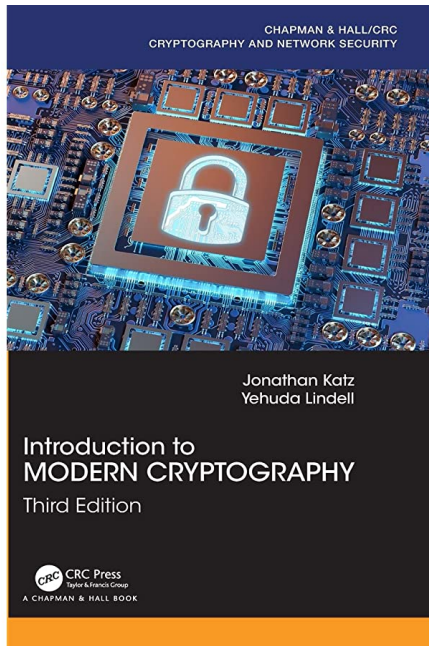
- Discuss how cryptography helps to achieve common **security goals** and tasks.
- Explain the notions of **core cryptographic primitives**, both **symmetric**, such as symmetric encryption, hash functions and message authentication codes, and **asymmetric**, such as public-key encryption and digital signatures.
- Sketch **formal security definitions** and describe prominent **implementation techniques** for such primitives and illustrate the difference between **symmetric Vs. asymmetric** cryptography.
- 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 asked questions or leading discussions 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 (independently or in small groups) on a final project. Final projects will take the form of handing in a report and giving a short presentation in class towards the end of the course. Projects types and 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 technologies, implementation of

specific security tools, analysis of real-world cyber attacks, or presentation of special topics of interest. More information about the logistics will be provided in class - e.g., about team formation, suggested topics, exact format, general timeline, involved deadlines, etc.

Late Assignment Policy

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

Late submissions are accepted but subject to the following rules:

- Each student has three 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 submission comes at 7am the following morning, then the student necessarily uses one (of the three) "late" days.
- After all three "late" days have been used, the following late-submission policy comes in effect:
 - Each (extra, automatically) 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 attendance and participation in class, 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	Sections 1.1, 1.2, 1.4 & corresponding lecture notes (https://sit.instructure.com/courses/63167/files/11115264?wrap=1)  (https://sit.instructure.com/courses/63167/files/11115264/download?download_frd=1)	-
1, 1/24	Course logistics, symmetric-key encryption, principles of modern cryptography		
	Symmetric-Key Encryption	Sections 2.1 - 2.3 & corresponding lecture notes (https://sit.instructure.com/courses/63167/files/11115264?wrap=1)  (https://sit.instructure.com/courses/63167/files/11115264/download?download_frd=1)	-
2, 1/31	Perfect secrecy, the One-Time Pad encryption and its analysis		
	Towards Practical Ciphers		
3, 2/07	Computational security, negligible functions, computational secure encryption, pseudorandom generators (PRG) and stream ciphers, pseudorandom functions (PRF) and block ciphers, chosen-plaintext attacks and CPA-security	Sections 3.1 - 3.6 & corresponding lecture notes	HW1
	Provable Security		
4, 2/14	Proofs by reduction, an EAV-secure fixed-length encryption scheme and its security proof	Sections 3.3.2 - 3.3.3 & corresponding lecture notes	-
	Message Integrity		
5, 2/21	Message integrity, MACs, generic MAC constructions (fixed-length	Sections 4.1 - 4.5 & corresponding lecture notes	HW2

MAC, domain extension for MACs,
CBC-MAC, authenticated
encryption

2/28 ***No Class (Monday Schedule)***

Hash Functions

6, 3/07	hash functions, Merkle-Damgård design framework, applications to MAC design, applications of hash functions to the design of MACs: The 'Hash & MAC' technique and its security analysis, HMAC, birthday attacks, the random oracle model	Sections 5.1 - 5.6 & corresponding lecture notes	Project Ideas
----------------	---	--	---------------

3/14 ***No Class (Spring Break)***

DH Key Agreement

7, 3/21	Practical constructions of symmetric-key primitives (DES, AES, SHA2), the key agreement problem, the discrete log problem and the DH key-agreement protocol	Sections 6.1 - 6.3, 8.3, 10.3 and corresponding lecture notes
----------------	---	--

Public-key cryptography

8, 3/28	Number theory, cryptographic hardness assumptions, motivation for public-key cryptography, key management, PK encryption and digital signatures	Sections 8.1 - 8.3, 10.1 - 10.4, 11.1, 12.1 and corresponding lecture notes	HW3
----------------	---	--	-----

	Public-key encryption & signatures	
9, 4/04	Hybrid encryption, El Gamal encryption, the RSA algorithm and cryptosystem, plain RSA, padded RSA, PKCS extensions	Sections 11.2 - 11.5, 12.2 - 12.4 and corresponding lecture notes
10, 4/11	Special Topics II (Revision)	TBD
11, 4/18	Special Topics III	TBD
12, 4/25	Special Topics IV	TBD
13, 5/02	<i>Project Presentations</i>	
14, 5/??	<i>Project Presentations</i>	

Academic Integrity

This is a 500-level course, thus governed by three academic integrity policies which are described below.

- 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.

(1) Undergraduate Honor System

Enrollment into the undergraduate class of Stevens Institute of Technology signifies a student's commitment to the Honor System. Accordingly, the provisions of the Stevens Honor System apply to all undergraduate students in coursework and Honor Board

proceedings. It is the responsibility of each student to become acquainted with and to uphold the ideals set forth in the Honor System Constitution. More information about the Honor System including the constitution, bylaws, investigative procedures, and the penalty matrix can be found online at <http://web.stevens.edu/honor/> ➞ [\(http://web.stevens.edu/honor/\)](http://web.stevens.edu/honor/)

The following pledge shall be written in full and signed by every student on all submitted work (including, but not limited to, homework, projects, lab reports, code, quizzes and exams) that is assigned by the course instructor. No work shall be graded unless the pledge is written in full and signed.

"I pledge my honor that I have abided by the Stevens Honor System."

Reporting Honor System Violations

Students who believe a violation of the Honor System has been committed should report it within ten business days of the suspected violation. Students have the option to remain anonymous and can report violations online at www.stevens.edu/honor ➞ [\(http://www.stevens.edu/honor\)](http://www.stevens.edu/honor/).

(2) Graduate Student Code of Academic Integrity

All Stevens graduate students promise to be fully truthful and avoid dishonesty, fraud, misrepresentation, and deceit of any type in relation to their academic work. A student's submission of work for academic credit indicates that the work is the student's own. All outside assistance must be acknowledged. Any student who violates this code or who knowingly assists another student in violating this code shall be subject to discipline.

All graduate students are bound to the Graduate Student Code of Academic Integrity by enrollment in graduate coursework at Stevens. It is the responsibility of each graduate student to understand and adhere to the Graduate Student Code of Academic Integrity. More information including types of violations, the process for handling perceived violations, and types of sanctions can be found at www.stevens.edu/provost/graduate-academics ➞ [\(http://www.stevens.edu/provost/graduate-academics\)](http://www.stevens.edu/provost/graduate-academics/).

(3) Special Provisions for Undergraduate Students in 500-level Courses

The general provisions of the Stevens Honor System do not apply fully to graduate courses, 500 level or otherwise. Any student who wishes to report an undergraduate for a violation in a 500-level course shall submit the report to the Honor Board following the protocol for undergraduate courses, and an investigation will be conducted following the same process for an appeal on false accusation described in Section 8.04 of the Bylaws of the Honor

System. Any student who wishes to report a graduate student may submit the report to the Dean of Graduate Academics or to the Honor Board, who will refer the report to the Dean. The Honor Board Chairman will give the Dean of Graduate Academics weekly updates on the progress of any casework relating to 500-level courses. For more information about the scope, penalties, and procedures pertaining to undergraduate students in 500-level courses, see Section 9 of the Bylaws of the Honor System document, located on the Honor Board website.

Exam Room Conditions

No formal examination is used in this course.

Learning Accommodations

Stevens Institute of Technology is dedicated to providing appropriate accommodations to students with documented disabilities. The Office of Disability Services (ODS) works with undergraduate and graduate students with learning disabilities, attention deficit-hyperactivity disorders, physical disabilities, sensory impairments, psychiatric disorders, and other such disabilities in order to help students achieve their academic and personal potential. They facilitate equal access to the educational programs and opportunities offered at Stevens and coordinate reasonable accommodations for eligible students. These services are designed to encourage independence and self-advocacy with support from the ODS staff. The ODS staff will facilitate the provision of accommodations on a case-by-case basis.

Disability Services Confidentiality Policy: Student Disability Files are kept separate from academic files and are stored in a secure location within the Office of Disability Services. The Family Educational Rights Privacy Act (FERPA, 20 U.S.C. 1232g; 34CFR, Part 99) regulates disclosure of disability documentation and records maintained by Stevens Disability Services. According to this act, prior written consent by the student is required before our Disability Services office may release disability documentation or records to anyone. An exception is made in unusual circumstances, such as the case of health and safety emergencies.

For more information about Disability Services and the process to receive accommodations, visit <https://www.stevens.edu/office-disability-services>. If you have any questions please contact: Phillip Gehman, the Director of Disability Services Coordinator at Stevens Institute of Technology at pgehman@stevens.edu or by phone (201) 216-3748.

Inclusivity

- **Name and Pronoun Usage**

- As this course includes group work and in-class discussion, it is vitally important for us to create an educational environment of inclusion and mutual respect. This includes the ability for all students to have their chosen gender pronoun(s) and chosen name affirmed. If the class roster does not align with your name and/or pronouns, please inform the instructor of the necessary changes.

- **Inclusion Statement**

- Stevens Institute of Technology believes that diversity and inclusiveness are essential to excellence in academic discourse and innovation. In this class, the perspective of people of all races, ethnicities, gender expressions and gender identities, religions, sexual orientations, disabilities, socioeconomic backgrounds, and nationalities will be respected and viewed as a resource and benefit throughout the semester. Suggestions to further diversify class materials and assignments are encouraged. If any course meetings conflict with your religious events, please do not hesitate to reach out to your instructor to make alternative arrangements.
- You are expected to treat your instructor and all other participants in the course with courtesy and respect. Disrespectful conduct and harassing statements will not be tolerated and may result in disciplinary actions.

Mental Health Resources

Part of being successful in the classroom involves a focus on your whole self, including your mental health. While you are at Stevens, there are many resources to promote and support mental health. The Office of Counseling and Psychological Services (CAPS) offers free and confidential services to all enrolled students who are struggling to cope with personal issues (e.g., difficulty adjusting to college or trouble managing stress) or psychological difficulties (e.g., anxiety and depression). Appointments are strongly encouraged and can be made by phone (201-216-5177) or in-person (on the 7th floor of the Howe Center). CAPS is open from 9:00 am – 5:00 pm Mondays, Wednesdays, Thursdays and Fridays and from 9:00 am – 7:00 pm on Tuesdays during the Fall and Spring semesters.

Emergency Information

In the event of an urgent or emergent concern about the safety of yourself or someone else in the Stevens community, please immediately call the Stevens Campus Police at 201-216-5105 or on their emergency line at 201-216-3911. These phone lines are staffed 24/7, year round. Other 24/7 resources for students dealing with mental health crises include the National Suicide Prevention Lifeline (1-800-273-8255) and the Crisis Text Line (text “Home” to 741-741). If you are

concerned about the wellbeing of another Stevens student, and the matter is *not* urgent or time sensitive, please email the CARE Team at care@stevens.edu (<mailto:care@stevens.edu>). A member of the CARE Team will respond to your concern as soon as possible.