AMERICAN
UNIVERSITY
OF BEIRUT

Applied Cryptography

CMPS 297AD/396AI, Fall 2025

Instructor: Nadim Kobeissi **Website:** https://appliedcryptography.page

Course Syllabus

Applied Cryptography explores the core theory of modern cryptography and how to apply these fundamental principles to build and analyze real-world secure systems. We start with foundational concepts—such as Kerckhoff's Principle, computational hardness, and provable security—before moving on to key cryptographic primitives like pseudorandom generators, block ciphers, and hash functions. Building on this solid groundwork, we will survey how these technologies power critical real-world deployments such as TLS, secure messaging protocols (e.g., Signal), and post-quantum cryptography. We will also delve into specialized topics like high-assurance cryptographic implementations, elliptic-curve-based systems, and zero-knowledge proofs to give you a complete understanding of contemporary cryptography's scope and impact. By the end of the semester, you will have gained both a rigorous theoretical perspective and practical hands-on experience, enabling you to evaluate, design, and implement cryptographic solutions.

1 Course Objectives & Outcomes

This course is designed to bridge the theoretical foundations of cryptography with its practical applications in contemporary secure systems. By engaging with lectures, lab sessions, problem sets, and project work, you will develop a thorough understanding of modern cryptographic concepts and gain the hands-on skills needed to implement, assess, and communicate security solutions.

Upon successful completion of this course, a student should be able to:

- Understand the reasoning behind the mathematical underpinnings of modern cryptography.
- Analyze and prove the security properties of cryptographic constructions.
- Understand how cryptographic constructions can be composed to build secure protocols and systems.
- Discern between how cryptography is approached mathematically versus from an engineering perspective.
- Critically assess security implementations and evaluate real-world cryptographic protocols.
- Gain an understanding about the future of cryptography and its role in emerging technologies.

2 Course Prerequisites

This course is intended for **senior undergraduate** students. **Graduate students** are also welcome to register provided that they are working on a research topic that is relevant to this course. The following prerequisites are **optional but recommended**:

- **CMPS 215:** Theory of Computation

If you want to understand whether you have the sufficient background for this course, review this revision chapter and try to do all the exercises: https://joyofcryptography.com/pdf/chap0.pdf

3 Materials

- Mike Rosulek, *The Joy of Cryptography*, Oregon State University, 2021.[1]
- Handouts will be made available during the course and on the course website.

[1] *The Joy of Cryptography* is available free of charge at https://joyofcryptography.com.

4 Course Schedule

The course schedule is available on the course website, where it is always kept up-to-date, including details about the lecture topics, materials and easy access to slides: `https://appliedcryptography.page`

5 Assessment Items & Grading Criteria

In this course, your performance will be evaluated through multiple components designed to measure both your theoretical understanding and your practical skills in cryptography. By staying current with the readings, attending and participating in lectures and lab sessions, and completing all assigned work, you will gain a thorough mastery of the material.

Overall, these graded components are designed to ensure that you not only grasp the theoretical underpinnings of cryptography but also develop the practical expertise needed to implement, analyze, and innovate within the field.

5.1 This Is Your Classroom

An essential facet in this course's design is encouraging students to produce work that is entirely theirs, without resorting to AI technologies. This ensures that students are embracing their full learning potential and makes grading more fair throughout the classroom. As such, the class sessions and lab sessions will favor **engagement**:

- **Interactive lectures:** Classes will incorporate interactive elements such as in-class exercises, discussions, and collaborative problem-solving to encourage active participation.
- **Real-time feedback:** Students will regularly have opportunities to demonstrate their understanding through low-stakes activities, receiving immediate feedback to guide their learning.
- **Peer teaching:** Students will occasionally be invited to explain concepts to their peers, reinforcing their own understanding while creating a collaborative learning environment.
- **Lab progress discussions:** Students will be encouraged to openly discuss their progress on lab projects as they work, allowing for real-time problem-solving and knowledge sharing.
- **Security strategy workshops:** During lab sessions, students will present their approaches to implementing security goals, receiving feedback from peers and instructors to refine their solutions.
- **Collaborative troubleshooting:** Labs will incorporate structured time for students to collectively address challenges, fostering a community where security insights and implementation techniques are freely exchanged.

5.2 Problem Sets

Problem sets will be assigned periodically throughout the semester to reinforce and deepen your understanding of the lecture material. Each set will include a range of exercises—some focused on theoretical proofs and problem-solving, others requiring short coding tasks or computational experiments. These assignments are designed to bridge the gap between abstract cryptographic concepts and their concrete applications. You are encouraged to start working on each problem set early and to seek guidance during office hours or lab sessions if you encounter difficulties.

5.3 Lab Sessions

Weekly lab sessions will be held to serve as a hands-on complement to the lectures. During each lab, you will experiment with real-world libraries, and even simulate attacks or vulnerabilities to understand why certain security practices are necessary. These sessions will also help you become comfortable with relevant tools and environments, including formal analysis tools. Attendance is mandatory, and lab participation will be graded based on preparedness, engagement, and the successful completion of in-lab activities. Labs offer an excellent opportunity for collaborative problem-solving and immediate feedback on your work.

Example lab sessions include:

- **Zero-Knowledge Battleship:** Build a secure battleship game that uses zero-knowledge proofs to verify that the server is reporting ship hits honestly without revealing the entire board layout. This lab explores ZKP implementations and demonstrates their power in creating trustworthy interactive applications.
- **Cryptographic Protocol Reverse Engineering:** Analyze real-world mobile applications to identify how they implement cryptographic protocols, discover potential vulnerabilities, and understand how protocol design flaws can lead to security breaches.
- **Breaking Cloud Storage Encryption:** Investigate current research into vulnerabilities in cloud storage encryption protocols. Implement proof-of-concept attacks in a controlled environment and propose mitigations for the discovered vulnerabilities.
- **Implementation of Secure Messaging Protocols:** Implement a simplified version of the Signal Protocol for secure messaging, focusing on the Double Ratchet algorithm and how it provides forward secrecy and post-compromise security.
- **Side-Channel Attack Workshop:** Perform practical timing and power analysis attacks against basic cryptographic implementations to understand the importance of constant-time algorithms and other side-channel mitigations.
- **Post-Quantum Cryptography Evaluation:** Compare and test different post-quantum cryptographic algorithms, analyzing their performance, security margins, and implementation challenges.
- **Formal Verification with Verifpal, Progressing to Tamarin:** Model cryptographic protocols first using Verifpal as a learning tool and then progressing towards mature tools such as Tamarin, automatically verifying their security properties, learning how formal methods can discover subtle vulnerabilities that manual review might miss.

Lab participation will be graded based on preparedness, engagement, demonstrated understanding during checkpoints, and the successful completion of in-lab activities.

5.4 Exams

There will be a midterm exam and a comprehensive final exam. The exams will test your command of topics discussed throughout the semester. You are expected to come to each exam prepared, having thoroughly reviewed lecture notes, and lab material.

5.5 Grading Breakdown

The final course grade will be computed using the following breakdown:

Category	Percentage
Attendance & Participation	10%
Problem Sets	10%
Lab Sessions & Projects	30%
Midterm Exam	25%
Final Exam	25%

6 Course Policies

Students are expected to strictly observe the following course policies:

6.1 Attendance

Do not register for this course if you do not plan to attend all classes, labs, and exams. You are expected to abide by the university's rules on attendance. You are expected to attend lectures and to be on time for all sessions and activities related to this course. Lectures are a sequence. Missing one lecture will almost certainly mean that you will not be able to keep up with the following lectures without studying the material covered in the missed lecture. Catching up with missed lectures is your responsibility and is done on your own time. You are responsible for all work, even when absent. Attendance may be recorded at every class session. Excessive absence will not be tolerated and will result in being dropped from the course.

6.2 Academic Misconduct & Plagiarism

Lectures and labs start on time. You may not be allowed to come into the room or lab once class has started. Any class conduct that disturbs the learning atmosphere may be deemed misbehavior and will not be tolerated.

This course has a strict **zero tolerance policy for cheating**. Any instance of cheating will result in an immediate, non-negotiable grade of 0 on the pertinent assignment and a report to the university faculty:

- Your work has to be your own. No copying work (or rewriting it line by line based on someone else's work) will be tolerated.
- Any sharing of any answers on any assignment is considered cheating.
- Coaching another student by helping them writing their answers line by line is also cheating.
- Copying answers or code from the Internet or hiring someone to write your answers for you is cheating.

Explaining how to use systems or tools and helping others with high-level design issues is not cheating.

Regarding AI Tools: Any use of AI tools to produce answers to class assignments or lab projects is considered cheating.

- Using AI tools like ChatGPT, GitHub Copilot, or similar to generate code, proofs, or written answers constitutes cheating.
- Submitting AI-generated work without proper attribution and explanation is considered plagiarism.
- The course will employ AI-detection tools and manual review techniques to identify AI-generated submissions.
- Using AI to enhance your learning experience (e.g. asking ChatGPT questions about the material) is not considered cheating.

The Student Code of Conduct[2] acts as the main reference in determining instances of misconduct.

6.3 Communication Policy

You are requested to check your e-mail and the course website regularly. You are responsible for all the information communicated to you via these tools. **Bookmark the course website and visit it regularly. All course news will be kept up to date on the website.**

7 Note for Special Needs Students

AUB strives to make learning experiences as accessible as possible. If you anticipate or experience academic barriers due to a disability (including mental health, chronic or temporary medical conditions), please inform the course instructor immediately so that we can privately discuss options. In order to help establish reasonable accommodations and facilitate a smooth accommodations process, you are encouraged to contact the Accessible Education Office: accessibility@aub.edu.lb; +961-1-350000, x3246; West Hall, 314.

[2] https://www.aub.edu.lb/SAO/Documents/student%20code%20of%20conduct.pdf

8 Nondiscrimination

AUB is committed to facilitating a campus free of all forms of discrimination including sex/gender-based harassment prohibited by Title IX. The University's non-discrimination policy applies to, and protects, all students, faculty, and staff. If you think you have experienced discrimination or harassment, including sexual misconduct, we encourage you to tell someone promptly. If you speak to a faculty or staff member about an issue such as harassment, sexual violence, or discrimination, the information will be kept as private as possible, however, faculty and designated staff are required to bring it to the attention of the University's Title IX Coordinator. Faculty can refer you to fully confidential resources, and you can find information and contacts at `https://www.aub.edu.lb/titleix`. To report an incident, contact the University's Title IX Coordinator Trudi Hodges at 01-350000 ext. 2514, or titleix@aub.edu.lb. An anonymous report may be submitted online via EthicsPoint at `https://www.aub.ethicspoint.com`.