**Course:** ENPM657 – Applied Cryptography – Fall 2024
**Instructor:** Dr. Daniel Apon
**Email:** dapon@umd.edu

# Course Overview

This course is a graduate-level introduction to cryptography, whose aim is to present the foundations of cryptosystems used in the real world. We will look "under the hood" of modern cryptography to get an understanding of various cryptographic primitives, algorithms, attacks, and protocols. However, as compared to an undergraduate-level introductory course, we will touch on certain basic topics only briefly in order to include additional advanced topics from the modern practice of real-world cryptography – particularly from the rapidly-developing field of *post-quantum cryptography* (PQC) – in the latter part of the course.

The textbook for this course is *Introduction to Modern Cryptography (3rd Edition)* by Katz and Lindell. The third edition of the book is required, as it contains new material on PQC that we will cover in the course. Students are strongly advised to obtain a physical copy of the book since exams will be "open book and open notes" with no Internet searches / online reference material permitted. Note that (illegal) copies of the book available online often do not match the printed edition.

Additional course material will be supplied via guest lectures from multiple U.S. Government speakers in order to provide students in the course with a "first hand, front lines" point of view on the ongoing, wide-scale roll-out of PQC algorithms and protocols, and can only be fully obtained by live participation in-class (or virtually as permitted) in these lectures.

*This course has significant mathematical content.* A solid background in discrete mathematics (probability, statistics, modular arithmetic, basic linear algebra) is assumed. Students are also assumed to have "mathematical maturity" since many of the concepts will be in the form of abstract and rigorous definitions, proofs will be given, and some new mathematics (e.g., group theory, number theory, discrete Gaussian sampling theory) will be introduced as needed. A basic familiarity with computational complexity theory and reduction-style proofs (e.g., in the theory of NP-completeness) may serve as helpful but is not required.

*The homeworks in this course will require programming.* The choice of programming language is flexible, but C, Python, and Sage are highly recommended. It is assumed that you can independently pick up what you need regarding programming techniques in order to complete the assignments. Basic background in algorithms (big-O notation and worst-case analysis, reading pseudocode) is assumed.

Parts of this course will include the presentation of cryptanalysis (i.e., mathematical/computational attacks) based on quantum algorithms. A background in quantum computing will not be assumed.

# Grading

There will be a midterm exam and an applied, semester-long project (acting as final exam). The first part of the course (approximately the first 40% of the course) will cover "private-key cryptography," and the midterm exam will cover only this material. The remaining, second part of the course will cover "public-key cryptography," including PQC.

There will be two programming homework assignments before the midterm exam (one very easy, and one more difficult). There will be one programming homework assignment after the midterm exam (moderate difficulty). Working in groups of 2 with another student in the course is allowed for programming assignments, but you *must declare* who you worked with. We will agree on groups for homeworks ahead of time.

There will be at least five online quizzes (at least two before the midterm, and at least three after), which are intended to be "quick" online exercises in between lectures. (Quizzes should take 10-20 minutes each.) The main purpose of quizzes is to gauge how the class is learning/understanding the material, to reinforce key concepts, and for the instructor to see how to make corrections in presentation as needed. Extra points from quizzes also helps dilute how damaging a mistake on an exam question might be.

Summarizing, grades will be based on:

1. Five or more quizzes – no collaboration allowed; Internet searches & book/notes allowed. (25%)
2. Three programming homework assignments – perhaps in a group. (25%)
3. A midterm exam – no collaboration/Internet searches allowed; "open book and open notes." (20%)
4. A major, semester-long, applied implementation-of-cryptography project; i.e. "the final exam." (30%)

# Tentative Course Schedule

## • Part Zero – Introduction to Cryptography

0. Monday, August 26
    - A brief history of cryptography (1945 B.C. - 1945 A.D.), the Vigenère cipher, the One-Time Pad
        † Homework 1 assigned
1. Monday, September 2
    - LABOR DAY – No class this week

## • Part One – Private-Key Cryptography

2. Monday, September 9
    - Computational security / indistinguishability, pseudorandomness, PRGs
        † Discussion of semester project; plan to finalize project idea within 2 weeks
3. Monday, September 16
    - CPA-security, PRFs, PRPs, AES
        † Homework 1 due before class meets
4. Monday, September 23
    - Modes of encryption, stream/block ciphers, MACs
5. Monday, September 30
    - Malleability, CCA-security, padding oracle attacks, secure sessions
        † Homework 2 assigned
6. Monday, October 7
    - Hash functions, birthday attacks, Merkle-Damgård, the random oracle model, SHA-2 / SHA-3
        † Guest short-lecture by Ray Perlner (NIST Crypto) on Hash Functions
        † Practice midterm exam posted & some discussion in class

7. Monday, October 14
    - Brief in-class review and Q&A
    - **Midterm exam**, in class.
        † Homework 2 due before class meets for the Midterm exam

# • Part Two – Public-Key Cryptography

8. Monday, October 21
    - Computational number theory, the {RSA, discrete logarithm, Diffie-Hellman} problems
9. Monday, October 28
    - New directions in cryptography, key exchange, public-key encryption, the RSA cryptosystems, digital signatures, hash-and-sign, full-domain hashing, Fiat-Shamir
        † Homework 3 assigned
10. Monday, November 4
    - The need for PQC (intro to quantum computing & Shor's algorithm); "harvest now, decrypt later"
        † Guest half-lecture by John Kelsey (NIST Crypto) on Hash-based Signatures
11. Monday, November 11
    † Guest half-lecture by Dr. Maxime Bros (NIST Crypto) on Code-Based Cryptography
    - Lattice-based cryptography, part I
        † Homework 3 due before class meets
12. Monday, November 18
    - Lattice-based cryptography, parts II and III
13. Monday, November 25
    - Lattice-based cryptography, part IV
        † Guest half-lecture by Ray Perlner (NIST Crypto) on Lattice Signatures
    - Wrap-up of Parts One and Two: How to talk with strangers on the Internet (the TLS protocol)

# • Part Three – Advanced Topics in Cryptography

14. Monday, December 2
    - Introduction to Fully Homomorphic Encryption / "Computing on Encrypted Data"
15. Monday, December 9
    - Course wrap-up – Advanced topic TBD based on students' interests

# • End of Course Events

- Monday, December 16 – Noon, Washington D.C. Time – Final Project Deliverables due via email

# General Information

- The class meets Mondays from 1:00pm to 3:40pm in JMP 2222. (Room to be confirmed later..)
- This course is **not curved**. What this means is that there is no predetermined number of students who will get As, Bs, Cs, etc. This also means that *students in the course are not competing with each other*. Every student's final grade will be determined by how well he/she/they is able to demonstrate his/her/their understanding of the material, and the expectation is that every student can be potentially get an A. The plus/minus grading system will be used.
- Homework policy:
  - You may collaborate on the homeworks with at most one other student in the class. Each student must independently write up their own solutions/code, and must list the other student (if any) with whom they collaborated.
  - You may consult **any** outside reference when doing the homework, so long as:
    * The sources you reference are properly cited in your homework submission;
    * You write up the solution yourself; and
    * *You understand the answer.*
  - Feel free to use ChatGPT however you want. Note that LLMs tend to perform **very** poorly on cryptographic challenges.
- Quiz policy:
  - Your work must be your own. Do **not** collaborate with classmates on quizzes.
  - Quizzes will be announced in class and posted on the course website (available for up to a week).
- Semester project (the "final exam"):
  - The semester project is due (submitted via email to the instructor) at Noon on Monday, December 9, 2024.
  - You are *encouraged* to collaborate in a group of two (2) to three (3) students for this work.
  - We will work out the nature/details/rules of this project at the beginning of the semester. It is every students' responsibility to make sure this is in writing (email or otherwise) by 11:59pm on Monday, September 23.
- Office Hours
  - The instructor, Dr. Daniel Apon, will have informal office hours for 20 minutes after every lecture, and also by appointment.
  - Students are **strongly encouraged** to ask for additional office hours / chats / conversations on a call (MS Teams, Zoom, Google Meet, etc.). The instructor will (happily!) attempt to schedule a meeting at a mutually suitable time within 2-3 days for most reasonable requests like this.
- Late Submission Policy
  - Late submissions will lose points at the discretion of the instructor. (Typically, accumulating -10% per 24 hour window.) No extensions will be granted without a valid excuse (e.g., religious/medical considerations), which should be discussed with the instructor in advance whenever possible.
- Last comments
  - My primary interest is in *you learning the material and concepts.* Cryptography is a very difficult topic – *[[insert commentary about the brutally-objective nature of the universe, hard mathematics, and so on]].* My Job #1 is to make cryptography as easy on you and fun for you as possible.
  - For students that perform *exceptionally well* in this course, I am happy to give/write recommendations for job/work positions in the field, connect you with people/companies, etc.
  - Good luck, and please enjoy! This really can be exciting stuff!