Course: ENPM657 – Applied Cryptography – Fall 2023
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 required 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 mechanics or quantum computing will not be assumed (nor required to learn), but may be helpful as well.

Grading

There will be a midterm exam and a 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, and the final exam will cover all material in the course (with emphasis on the latter 60% of material).

There will be two programming homework assignments before the midterm exam (one easy, one hard). There will be two programming homework assignments after the midterm exam (one moderately hard, one very hard). Working in groups of 2 with another student in the course is allowed for programming assignments, but you *must declare* who you worked with; submissions are individual.

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 20-30 minutes each.)

Once during the semester (with submission available anytime, but due before the final lecture on December 8, 2023), students will be expected to pick a modern research paper in cryptography (*ideally* from an IACR conference such as CRYPTO, EUROCRYPT, etc.; or IEEE's S&P; or ACM's CCS; which has been published within the past decade) and write a detailed technical summary of the paper in 4-5 pages in LaTeX. Students are encouraged to work in groups of 2-4 to read this paper and write their report. Points will be awarded based on demonstrating an understanding of the material and its context in the academic cryptographic literature (citing additional papers and technical matter referenced by the selected paper is an obvious plus).

Summarizing, grades will be based on:

1. One written report (4-5 pages, LaTeX) on modern cryptography research – perhaps in a group. (15%)
2. Five or more quizzes – no collaboration allowed; Internet searches & book/notes allowed. (15%)
3. Four programming homework assignments – perhaps in a group. (20%)
4. A midterm exam – no collaboration/Internet searches allowed; "open book and open notes." (20%)
5. A final exam – no collaboration/Internet searches allowed; "open book and open notes." (30%)

Tentative Course Schedule

• Part One – Private-Key Cryptography

1. Friday, Sept 1
   - A brief history of cryptography (1945 B.C. - 1945 A.D.), the Vigenère cipher, the One-Time Pad
2. Friday, Sept 8
   - Computational security / indistinguishability, pseudorandomness, PRGs

     † Homework 1 assigned
3. Friday, Sept 15
   - CPA-security, PRFs, PRPs, AES

     † Homework 1 due before class meets
4. Friday, Sept 22
   - **This single lecture will be VIRTUAL (held on Zoom).**
   - Modes of encryption, stream/block ciphers, MACs
5. Friday, Sept 29
   - Malleability, CCA-security, padding oracle attacks, secure sessions

     † Homework 2 assigned
6. Friday, Oct 6
   - Hash functions, birthday attacks, Merkle-Damgård, the random oracle model, SHA-2

     † Practice midterm exam posted
7. Friday, Oct 13
   - Brief in-class review and Q&A
   - **Midterm exam**, in class.

     † Homework 2 due before class meets

• Part Two – Public-Key Cryptography

8. Friday, Oct 20
    - Computational number theory, the {RSA, discrete logarithm, Diffie-Hellman} problems
9. Friday, Oct 27
    - 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. Friday, Nov 3
    - The need for PQC (survey of quantum computing & Shor's algorithm); "harvest now, decrypt later"
    - Guest half-lecture on (Stateful) Hash-Based Cryptography by John Kelsey,
a Computer Scientist at the National Institute of Standards and Technology (NIST)
11. Friday, Nov 10
    - Guest half-lecture on Code-Based Cryptography by Dr. Maxime Bros,
a Mathematician at the National Institute of Standards and Technology (NIST)
    - Lattice-based cryptography, part I
        - † Homework 3 due before class meets
12. Friday, Nov 17
    - Lattice-based cryptography, parts II and III
        - † Homework 4 assigned
13. Friday, Dec 1
    - Lattice-based cryptography, part IV
    - Guest half-lecture (tentative) on Internet protocols using PQC by Rebecca Guthrie,
an employee at the Center for Cybersecurity Standards (CCSS), National Security Agency (NSA)
14. Friday, Dec 8
    - Fully Homomorphic Encryption ("Computing on Encrypted Data"), and course wrap-up
        - † Homework 4 due before class meets
        - † Semester report project due before class meets
        - † Practice final exam posted

• End of Course Events

- Monday, Dec 11 – Special "long office hours" on Zoom in the afternoon and/or evening
- Tuesday, Dec 12 – Reading Day
- Friday, Dec 15 – Likely date for the **Final exam**, in person. (Date is NOT confirmed yet)

General Information

- The class meets Fridays from 1:00pm to 3:40pm in JMP 2222.
- 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:
  - Late homeworks **will not be accepted** without advance approval of the instructor.
  - 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.*
  - 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.
  - Feel free to use ChatGPT however you want; good luck..
- 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).
  - Late submission of quizzes **will not be accepted** without advance approval of the instructor.
- Semester's written-report-project policy:
  - The semester report is due (submitted online) at 1:00pm on December 8, 2023.
  - Late report submissions **will not be accepted** without advance approval of the instructor.
  - You are *encouraged* to collaborate in a group of two (2) to four (4) students for this work. The group may submit a single report to the Teaching Assistant, listing the names of students in the group.
  - We will work out which papers for this project (suggesting lists of papers to read, and verifying selections of papers for individuals/groups) in the first part of the course; the TA will facilitate this process.
- The Teaching Assistant and grader for the course is Narayan-Ram Narayanan.
  - His email is `nana2011@umd.edu`. Please preface your subject line with "[ENPM657] ..." when you email him. He will aim to respond within 48 hours.
  - He will host regular office hours on Zoom from 3pm-5pm on every Tuesday. The Zoom link will be provided in class. Additional office hours or a schedule adjustment may be possible during the semester based on students' needs.
  - The professor, Daniel Apon, will have informal office hours for 20 minutes after every lecture, and also by appointment. Please ask the TA Narayan your questions first (he is your first stop), and I will be available and happy to follow-up if anything remains unclear.
    Please email in advance of when you plan to request any additional office hours.
- Good luck, and please enjoy!