Syllabus CMSC-MATH-ENEE 456 Cryptology

This document has three parts with three very different functions.

- CONTENT: What is the content of the course.
- POLICY: How the course is run (office hours, tests, HW, etc). This will be particular to this course.
- GENERAL INFO: This information is helpful for any course you take at UMCP. It is not geared towards this course.

CONTENT

THEME: Alice wants to send Bob a message. Eve can eavesdrop. Hence Alice sends her message in code that Bob can decode. How can they do this so Eve cannot crack the code? How can Alice prove that she is Alice? We study these and related issues in a rigorous framework. The list below is approximate in many ways. Some topics may end up not being covered. Some may be for more or less lectures than indicated.

1. Classical Cryptography: Shift, Affine, Vigenere, Matrix, 1-time pads, breaking random generators, (4 lectures)
2. Public Key Cryptography based on Number Theory: Diffie Helman, ElGamal, RSA. (4 lectures)
3. Number Theory Algorithms to break Public Key. (3 lectures)
4. Public Key Cryptography NOT based on Number Theory (called *post-quantum*). Learning with Errors (2 lectures)
5. Digital Signatures and Authentication (2 lectures)
6. (2 lectures) Cryptographic Hash Functions and their applications
7. Pseudo Random Generators (2 lectures)
8. Secret Sharing (3 lectures)
9. Guest lecture on censorship. (Not scheduled yet.) (1 lecture)
10. Guest lecture on the NIST post-quantum challenge. (Not scheduled yet.) (1 lecture)

Possible other topics

1. The Quadratic Sieve Factoring Algorithm.
2. Message Authentication Codes (MAC).
3. Feistel Networks, MD5, AES, DES and other Real Systems

REQUIRED TEXT There is no text. There will be notes on line and slides on line.

RECOMMENTED TEXT Introduction to Cryptography and Coding Theory by Trappe and Washington.

PREREQUISITES (CMSC 106 OR CMSC 131 OR ENEE 150 OR Equiv Prog Exp) AND ((2 from CMSC 330, CMSC 351, ENEE 324, ENEE 380) OR (any of those and a 400-level MATH course) OR (two 400 level MATH courses) OR Permission of instructor.

POLICY

1 Basic Information

Course title and Number CMSC-MATH-ENEE 456. Cryptology.
Term: Fall 2021
Credits: 3
Course Dates: Aug 31-Dec 9. No class Nov 25 (Thanksgiving)
Class Time and Place Tu-Th 12:30-1:45. Room IRB 0318.
Course Website `http://www.cs.umd.edu/~gasarch/COURSES/456/F21/index.html`
ELMS Elms will have the recordings of the lectures. Only students from this class will have access to it.
Gradescope You will submit HW on gradescope and this is where you can see your grades and make re-grade requests.

2 Course Guidelines

Academic Integrity for CMSC-MATH-ENEE 456

1. **Non-programming Homework Assignments** You may talk to your fellow students about the problems however you must hand in your own work and you must understand your own work.

2. **Programming Homework Assignments** You may talk to your fellow students but you may not exchange any code.

3. **Optional Project** Like the Non-Programming HW.

4. **Exams** These must be solely your own work.

Communication from you to the instructor or TAs You should feel free to email us or post things on piazza or meet us in office hours. You can also request a zoom meeting if that makes more sense.
Communication from us to you We will email you (1) when HWs are posted, (2) when HW solutions are posted, and (3) other things you need to know. We will respond to your piazza posts promptly.

3 Homework, Exams, Optional Project, and Grading

For all of the below see the Academic Integrity section above for guidance on how much help you can get on the Homework, Exams, and Optional Project.

1. **Homework** There will be problems and short programming assignments based on the material. They will be roughly once a week. The Homework will be posted on the course website (NOT on elms) in three forms. We do an example with hw00.

   hw00.pdf

   hw00st.txt- this is plaintext

   hw00st.tex- this is LaTeX

   You may use the .txt or .tex to help you typeset your homework.

   After the Dead-Cat day has passed (see later for what that means) I will post hw00sol.pdf- Solutions to some of the problems.

   Typed Homework must be typed and submitted on gradescope. If diagrams are needed to be drawn they can be handwritten.

   Dead Cat Policy HW is posted on Tues and due the following Tues at 12:30PM. But *everyone* gets an extension to Thursday at 12:30PM. *Do not* think *the real deadline is Thursday.* I have already given you an extension to Thursday, hence I am not going to give you another one. I use the phrase **Morally due Tuesday Oct 19, 12:30**.

2. **Take Home Part of the Midterm** Morally Due Tue Oct 19, 12:30PM (before class) This will be given out the prior week so it can be viewed as a take-home exam.

3. **Timed Part of the Midterm** Thu Oct 28, 8:00PM-10:00PM. You will take it at home. I will post it at 8:00PM and you will have 2 hours to do it and post it on gradescope. It will be open-book, open-notes, open-web. You CANNOT ask another human being for help but, if your cat is still alive, you can ask them. (Exceptions for timeslot will be made for students who cannot do the exam in that timeslot.)

4. **Optional Project** After the midterm is graded and returned I will post an optional project which will be a long HW covering most of the class. It will be due the last day of class (no extension). *After* the entire course is graded and I have assigned initial letter grades I will look at those students who earned a D or F. If the optional project shows they understand the material on some level than I will bump their grade: A D can get bumped to a C-. An F can get bumped to a D. You can consider this insurance against getting a D or lower in the course. Since you have a long time to work on this it has to be very well written.

5. **Final** The final will be similar in format to the midterm, though the exact dates are not known yet.

4 Grading Structure

We will make each HW worth 4% of the grade. We intend to have 10 HW. That leads to the following table; however, if we have a different number of HW this will change slightly.

Homework	40%
Midterm	30%
Final	30%

Grades will be ROUGHLY

- 90-100 is an A
- 80-89 is a B
- 60-79 is a C
- 45-59 is a D
- 0-44 is an F.

Notice that (1) this is ROUGH- there may be some adjustments in any direction, and (2) this will be further refined with + and - after the final. academic dishonesty will be dealt with harshly.

Staff, Office Hours, email addresses

- Prof William Gasarch `gasarch@umd.edu` Office Hours Tuesday 2:00-5:00PM, Thursday 2:00-3:15; in his office, IRIBE 2242. also He is also usually around Tu-Th 11:00-12:15. You can also make an appointment. This can be very flexible, even at night, since we can use zoom:

  `https://umd.zoom.us/my/gasarch`

- TA Josh Twitty `jtwitty@terpmail.umd.edu` Office hours: Tu 3:30-5:30, in AV Williams 4166.
- TA Seyed Sajjad Nezhadi `sajjad@umd.edu` Office hours: Wed 5:00PM-7:00PM (thats 2 hours, not 14 hours) in AV Williams 4166.
- Kunal Mehta `kjmehta@terpmail.umd.edu` Office hours: Monday 5:00-6:00 in AV Williams 4166.

Note on Location of TA office hours for CS TAs These are set by the dept and are here: `http://www.cs.umd.edu/class/resources/cstarooms/fallspring/`

5 Course Evaluations

COURSE EVALUATIONS In Dec you will be asked to fill out course evals. I will urge you to fill out, not just the eval for me, but the eval for ALL of your courses. I have been on the committees that reads these evals and it is important that they be filled out.

GENERAL INFORMATION

UNIVERSITY POLICY We follow university policies. See
`https://www.ugst.umd.edu/courserelatedpolicies.html`

MASK POLICY Anyone in class must wear a mask that covers their nose and mouth. This is current university policy but also a very good idea. If the university policy changes then the class policy will also change.

Communication with the instructor or TAs You should feel free to email us or post things on piazza or meet us in office hours. You can also request a zoom meeting if that makes more sense.

6 UMD Policies and Resources for Undergraduate Courses

It is our shared responsibility to know and abide by the UMD policies that relate to all courses, which include topic like

- Academic Integrity
- Student and Instructor Conduct
- Accessibility and accommodations
- Attendance and excused absences
- Grades and appeals
- Copyright and intellectual property.

Please visit
`https://www.ugst.umd.edu/courserelatedpolicies.html`
for the UMCP policy on these issues.

7 Resources and Accommodations

7.1 Accessibility and Disability Services

The University of Maryland is committed to creating and maintaining a welcoming and inclusive educational, working, and living environment for people of all abilities. The University of Maryland is also committed to the principle that no qualified individual with a disability shall, on the basis of disability, be excluded from participation in or be denied the benefits of the services, programs, or activities of the University, or be subjected to discrimination. The Accessibility & Disability Service (ADS) (see here:)

`https://www.counseling.umd.edu/ads/`
provides reasonable accommodations to qualified individuals to provide equal access to services, programs and activities. ADS cannot assist retroactively, so it is generally best to request accommodations several weeks before the semester begins or as soon as a disability becomes known. Any student who needs accommodations should contact me as soon as possible so that I have sufficient time to make arrangements. For assistance in obtaining an accommodation, contact Accessibility and Disability Service at 301-314-7682, or email them at adsfrontdesk@umd.edu. Information about sharing your accommodations with instructors, note taking assistance and more is available from the Counseling Center.

7.2 Student Resources and Services

If you are not doing well in the course and want to do better feel free to talk to me so we can see what we can do. There are also campus services that might be helpful:
Tutoring and Academic Success `https://tutoring.umd.edu/`
UMD Writing Center `https://english.umd.edu/writing-programs/writing-center`
Website of Heath Services Websites `https://sph.umd.edu/academics/advising-resources/undergraduate-center-academic-success-and-achievement/casa-student-resources-and-information`

7.3 Basic Needs Security

If you have difficulty affording groceries or accessing sufficient food to eat every day or lack a safe and stable place to live, please visit
UMD Division of Student Affairs website `https://studentaffairs.umd.edu/basic-needs-security`
for information about resources the campus offers you.