CMSC 456 : CRYPTOGRAPHY
SPRING 2020
TUTH 2:00 - 3:15 IRB 0318
SYLLABUS

People

Instructor: Gorjan Alagic (galagic@umd.edu); office hours: by appointment (ATL 3102).
TAs:

- Elijah Grubb (egrubb@cs.umd.edu) 11am-12pm TuTh (Iribe)
- Justin Hontz (jhontz@terpmail.umd.edu) 1pm-2pm MW (Iribe)
- Chen Bai (cbai1@terpmail.umd.edu) 3:30-5:30pm Tu (2115 ATL, start Feb 4)
- Bibhusa Rawal (bibhusa@terpmail.umd.edu) 3:30-5:30pm Th (2115 ATL, start Feb 6)

Default TA location: open area across from IRB 5234. Check here for changes.

Resources

- Course page (check frequently for updates): alagic.org/cmsc-456-cryptography-spring-2020/
- Textbook: *Introduction to Modern Cryptography*, Katz and Lindell.
- Piazza: piazza.com/umd/spring2020/cmsc456
- Check ELMS for slides and assignments.
- We will be using Gradescope. Log into it via ELMS.
- Learning Assistance Services (www.counseling.umd.edu/LAS) Shoemaker 2202

Topics covered (tentative)

- *fundamentals of symmetric-key cryptography:* historical ciphers and cryptanalytic techniques, perfect secrecy and one-time pad, computational security, cryptographic pseudorandomness, CPA-secure encryption, CMA-secure authentication, block ciphers.
- *fundamentals of public-key cryptography:* public-key encryption, RSA, Diffie-Hellman, digital signatures, hash functions.
- *advanced topics:* some strict subset of: theoretical foundations of symmetric-key crypto, zero-knowledge proofs, post-quantum and quantum cryptography, Learning with Errors, fully-homomorphic encryption.

Key dates

- January: 28th (first lecture);
- February: 7th (add/drop);
- March: 17th and 19th (spring break); 26th (midterm review); 31st (midterm exam);
- April: 10th (W-drop);
- May: 12th (last lecture); 18th 10:30am-12:30pm (final exam).

Grading policy. The final grade will be 40% homework, 30% midterm exam, and 30% final exam. If you want to dispute a homework or exam grade you received, you must contact a TA or me within one week of receiving the grade. Please be mindful of matters of academic integrity, and the UMD course policies in general (see UMD course policies.)

We will likely be using Gradescope for grading homework assignments (and possibly also exams.)

Since this course is about a mathematically rigorous subject, here are some things to keep in mind when solving problems on homeworks and exams.

- All answers must be accompanied by complete and clear explanations. In some cases, the "explanation" will be a proof of some kind. A correct answer with no explanation will receive a zero score.
- Your goal in proofs is to convince the grader that, without any doubt, your answer is correct *and you understand why it is correct.* It is almost impossible to do this without at least some words. Those words should come in complete sentences.
- You must use clear, standard, and rigorous mathematical notation, following the examples set in lectures and the textbook.
- For open-ended questions, think carefully about what constitutes a proof that your response is correct. Sometimes, all it takes is a counterexample (and an explanation of why it is a counterexample.)

Exams. Exams are closed book. No electronic devices of any kind are allowed. You are allowed one double-sided page of handwritten notes, readable by an unassisted human. If you have to miss the exam, you must contact me with your explanation and evidence at least 48 hours in advance of the exam time.

Homework. There will be approximately 10 homeworks. They are due in class on the date specified on the homework set. *Late homework will not be accepted.* However, your lowest homework grade will be dropped when calculating the final grade. Use this "free pass" with caution: you only get one.

Collaboration is allowed, but each student must write up their own solutions individually, in their own words. If you want to use a theorem from the lectures or the book, you have to state it clearly or provide an unambiguous reference (e.g., "Theorem 1.17 on page 53 of Katz-Lindell.") If you want to use a theorem from outside lectures or the book (e.g., from a paper online), you have to provide a complete statement and a complete proof in your own words.

While collaboration is allowed, I strongly encourage you to spend some quality time studying the subject and doing the homeworks on your own. I recommend reasonably long (e.g., 25+ minute) chunks of uninterrupted time with no distractions. Take notes, work lots of examples (starting from the simplest ones you can imagine), and "play" with the new concepts until you develop an intuitive understanding of them.

Extra credit. There will be one additional homework set or project, which will be announced at a later time. This will be the only possibility for "rescuing" your grade.