Syllabus

Note: If you're reading the PDF version of this syllabus, you should switch to the HTML version online if possible. The PDF rendering of the original markdown has weirdness with lists, and none of the links to papers work in the PDF.

Course Info and Contact Information

- Course Name: CSE 539, Applied Cryptography (HYBRID)
- Instructor: Jed Crandall
- Email: jedimaestro@asu.edu
- Meeting Times: Certain Tuesdays 3:00pm to 4:15pm
- Meeting Location: Tempe - COORS 199
- Online Discussions: TBD (will probably be in Canvas or Piazza)

Office Hours

Time and location TBD

TAs

I'll announce the TA's name(s) and office hours early in the semester. Please do not contact the TA directly, all course-related communications with the TA should be through online discussion or office hours.

Course Description

"Uses cryptography for secure protocols over networked systems, including signatures, certificates, timestamps, electrons, digital cash, and other multiparty coordination." This is a direct quote from the catalog, note that "electrons" probably was intended to mean "elections".

Course Objectives

- Students will gain an understanding of symmetric cryptography and related attacks.
- Students will gain an understanding of asymmetric cryptography and related attacks.
- Students will gain an understanding of other concepts that are key to applied cryptography, including randomness, secure hash functions, and entropy.
- Students will gain a broad understanding of contemporary research topics in cryptography, including zero-knowledge proofs, blockchain, and private group chat.

Course Learning Outcomes

- Students will identify if a given cryptosystem is symmetric or asymmetric.
- Students will identify if a cryptosystem has perfect forward secrecy.
- Students will be able to compare two different cryptosystems or cryptographic protocols for security against a variety of symmetric and asymmetric attacks.
- Students will be able to compare the suitability of different industry-standard secure hash functions for different applications.
- Students will be able to compare the security of different random number generators.

Enrollment Requirements

Prerequisite(s): Computer Engineering or Computer Science graduate student OR Software Engineering MS student OR Online Computer Science nondegree-seeking graduate student

Grading Policies, Assignments, and Required Materials

The grade will be calculated as follows: - Attendance is 20% of the grade and will be self-graded, with a rubric that is described below. - Two homeworks (one assigned in late January and due in late February, the other assigned in late February and due in late March) are each 15% of the grade, for 30% total. - There will be a pre-exam early in the semester that is 10% of the final grade, but is an all-or-nothing grade based on participation where there are no wrong answers. - There will be a Final Exam that is worth 10% of the grade. It will probably be online. - There will be a final project worth 30% of the grade.

Rubric for attendance (10 points for each day broken up into 5 points for reading the assigned paper and 5 points for participating in discussion): - Reading... 5/5 if you read the paper carefully and took at least one note on every page, 3/5 if you ran out of time and skimmed it, 1/5 if you at least opened the PDF and looked at it. - Participation... 5/5 if you made at least one substantive comment in class or in the online discussion (both is okay), 3/5 if you followed the discussion (e.g., reading it or listening to it) online or in class, 1/5 if you at least showed up to class or opened the discussion board.

Final letter grades are based on the following scale where x is the percentage: 97.0 <= x <= 100.0 is an A+, 93.0 <= x < 97.0 is an A, 90.0 <= x < 93.0 is an A-, 87.0 <= x < 90.0 is an B+, 83.0 <= x < 87.0 is an B, 80.0 <= x < 83.0 is an B-, 77.0 <= x < 80.0 is an C+, 73.0 <= x < 77.0 is an C, 70.0 <= x < 73.0 is an C-, 60.0 <= x < 70.0 is D, and x < 60.0 is an E.

There is no textbook for the course, neither required nor recommended. All materials used for the course lectures and assignments will be widely and publicly available and/or licensed open source.

Absence policies and the conditions under which assigned work can be made up

Everyone is entitled to the following course-specific late policy for every homework assignment, but cannot combine it with any other form of absence forgiveness (e.g., any of them from below): For every hour that an assignment is turned in late, you will lose 1% of the grade. Note that a little after four days late the assignment is worth 0%.

As an alternative to that policy, for every course you are entitled to: - Excused absences related to religious observances/practices that are in accord with ACD 304-04. - Excused absences related to university sanctioned events/activities that are in accord with ACD 304-02. - Excused absences related to missed class due to military line-of-duty activities that are in accord with ACD 304-11.

In the event of an excused absence (which you must communicate with the instructor about), you can make up for the absence in your attendance grade by reading the paper and participating in the online discussion.

Instruction Style

The course will be a combination of recorded lectures that you can watch on your own time (but need to keep up on) and biweekly meetings to discuss papers.

Attendance and participation are required, but will not be recorded by the instructor or TA. You will self-grade based on the above rubric (i.e., the honor system).

For questions and answers regarding course materials and homework please use the course's discussion board or come to office hours, unless there is some compelling reason to use email. Use email for course administrativia (requesting an extension, you need a signature from me for some reason, etc.) Feel free to email me any time for anything, I won't shame you, but if you're asking questions about the homework or lectures you're much more likely to get a timely response in the course discussion platform than via email.

All homeworks should be done in Linux. You can use other OSes, but if you need help (tool recommendations, help with debugging, troubleshooting error messages, etc.) I will only try to help you with OS-specific things if you're using Linux.

You are responsible for your own file backups and time management. E.g., feel free email me, or send as a private post in Piazza, the day before something is due, "I worked on it all day and then my VM crashed and I lost my file!" I won't shame you, but that's not grounds for an extension and I'm not going to be able to do anything about it to make sure you submit your homework on time. I recommend keeping your code and other work for this course in a *private* repository (e.g., on github) that you periodically commit to.

Classroom Behavior

Please refrain from anything that will distract you or others from fully engaging in the class. Disruptive behavior will be dealt with according to university policies. While attendance and classroom behavior are not explicitly part of the grade, you are hereby notified that your attendance and classroom behavior are considered as part of your overall performance in the course to the extent allowed by university policies.

You may not record class discussions without permission.

Textbook

As stated above, no textbook is required for this course.

Course Topics (time invested in each is approximate)

- Intro to End-to-end encryption and Signal - 1 week
- PRNGs and randomness - 1 lecture
- Secure hash functions (MD5 collisions, SHA-3, etc.) - 2 weeks
- Block ciphers (Feistel structures like DES, SPNs like AES, linear and differential cryptanalysis) - 3 weeks
- Stream ciphers (RC4 and related attacks) - 1 week
- Diffie-Hellman - 1 week
- RSA + RSA-OAEP (and a QQ Browser attack example) - 2 weeks
- Elliptic curve crypto - 1 week
- Zero-knowledge proofs - 1 week
- Blockchain - 1 lecture
- Quantum and quantum-resistant crypto - 1 lecture
- Elections and other societal impact issues - 1 lecture

Assessment

Students will be evaluated on attendance and participation, their performance on homework assignments, and their performance on exams. Details are above.

Homework Due Dates

Homework due dates will be posted in advance on the class website and announced in class. All times will be Mountain Standard Time, i.e., Arizona time.

Course format

This is a HYBRID course where roughly 25% of the lecture time will be in-person discussions (these may or may not be recorded, and may or may not be available remotely over Zoom, depending on classroom constraints), and 75% of lecture time will be recorded lectures that I will post online. You are expected to keep

up with the recorded lectures at the same pace as if we were meeting every Tuesday and Thursday. I'll be explicit with every lecture announcement when you need to watch that lecture by.

Here is the schedule of in-person in-class meetings to discuss papers, and the papers we will discuss on each date: - January 10th - Introduction to the course - January 17th - Introduction to Signal and end-to-end crypto, and discuss the OTR paper - January 31st - Secure hash functions, and discuss this paper about MD5 collisions - Febrary 14th - Block ciphers, and discuss the MiniAES specification and a tutorial about linear and differential cryptanalysis - February 28th - Attacks on RC4 and the final nail in WEP's coffin - March 14th - Diffie-Hellman, and their classic paper March 28th - RSA, and their classic paper - April 11th - Reading and topic TBD - April 25th - Reading and topic TBD

Essentially, we will meet physically in the classroom the first day of classes, one week after that on January 17th, and then every other week from the 17th through the end of the semester.

Academic Integrity

Students in this class must adhere to ASU's academic integrity policy, which can be found at https://provost.asu.edu/academic-integrity/policy. Students are responsible for reviewing this policy and understanding each of the areas in which academic dishonesty can occur. In addition, all engineering students are expected to adhere to both the ASU Academic Integrity Honor Code and the Fulton Schools of Engineering Honor Code. All academic integrity violations will be reported to the Fulton Schools of Engineering Academic Integrity Office (AIO). The AIO maintains record of all violations and has access to academic integrity violations committed in all other ASU college/schools.

Plagiarism and Cheating Policies Specific to This Course

This course has a zero-tolerance policy: -Any violation of the academic integrity policy (detailed below) will lead to a failure on this course. -The violation will be reported to the AIO.

If you need more time to accomplish a homework assignment, please tell the instructor and ask for an extension. Extensions will be considered for circumstances that are/were beyond your control. Do not attempt plagiarism.

For this course, you are allowed to use code snippets that you find on the Internet as long as you specify clearly in the comment of your source code where the code snippets come from, and the source snippets existed before the assignment was assigned. You are not allowed to upload any part of your solution online or show it to other students. Using other students' answers or code, past or present, with or without a citation is seen as a violation of the academic integrity policy. You may or may not be asked to turn in your source code for any given assignment. In any case, if I suspect cheating I reserve the right to require you

to come to my office and show me a live demonstration of your source code and answer questions to get full points. Some assignments are graded automatically by grade scripts with anti-cheating mechanisms built-in. Do not cheat – it is not worth risking your grade and your academic profile.

Security token

As part of the first homework, you will generate or receive a 128-bit token that will serve as a sort of student ID for the course. You are not to make this token public; share it with any of your classmates; share it with anybody other than the instructor, yourself, and the TAs; find out the token of any of your classmates; or in any way compromise the confidentiality policy that only you yourself and the instructor/TAs for the course should know your security token. If you violate this policy that will be considered cheating as per the policy above.

Sexual Discrimination

Title IX is a federal law that provides that no person be excluded on the basis of sex from participation in, be denied benefits of, or be subjected to discrimination under any education program or activity. Both Title IX and university policy make clear that sexual violence and harassment based on sex is prohibited. An individual who believes they have been subjected to sexual violence or harassed on the basis of sex can seek support, including counseling and academic support, from the university. If you or someone you know has been harassed on the basis of sex or sexually assaulted, you can find information and resources at https://sexualviolenceprevention.asu.edu/faqs. As a mandated reporter, I am obligated to report any information I become aware of regarding alleged acts of sexual discrimination, including sexual violence and dating violence. ASU Counseling Services, https://eoss.asu.edu/counseling is available if you wish to discuss any concerns confidentially and privately. ASU online students may access 360 Life Services, https://goto.asuonline.asu.edu/success/online-resources.html.

Copyright

All course content and materials, including lectures (Zoom recorded lectures included), are copyrighted materials. You may not share outside the class, upload to online websites not approved by the instructor, sell, or distribute course content or notes taken during the conduct of the course. See ACD 304-06, "Commercial Note Taking Services" and ABOR Policy 5-308 F.14 for more information.

You must refrain from uploading to any course shell, discussion board, or website used by the course instructor or other course forum, material that is not the student's original work, unless the students first comply with all applicable copyright laws; faculty members reserve the right to delete materials on the grounds of suspected copyright infringement.

Policy Against Threatening Behavior

Students, faculty, staff, and other individuals do not have an unqualified right of access to university grounds, property, or services. Interfering with the peaceful conduct of university-related business or activities or remaining on campus grounds after a request to leave may be considered a crime. All incidents and allegations of violent or threatening conduct by an ASU student (whether on- or off-campus) must be reported to the ASU Police Department (ASU PD) and the Office of the Dean of Students.

Disability Accommodations

Suitable accommodations will be made for students having disabilities. Students needing accommodations must register with the ASU Disabilities Resource Center and provide documentation of that registration to the instructor. Students should communicate the need for an accommodation in sufficient time for it to be properly arranged. See ACD 304-08, Classroom and Testing Accommodations for Students with Disabilities.

Future Changes

Any information in this syllabus may be subject to change with reasonable advance notice.