Syllabus (Fall 2017)

1 Official Yale course listing

CPSC 467 01 (10727) /CPSC 567 01 (10728)
Cryptography and Computer Security
Michael Fischer
MW 1.00–2.15 AKW 200

Final exam scheduled (Group 36)
– 12/16/2017 S 7.00p
Skills QR

A survey of such private and public key cryptographic techniques as DES, RSA, and zero-knowledge proofs, and their application to problems of maintaining privacy and security in computer networks. Focus on technology, with consideration of such societal issues as balancing individual privacy concerns against the needs of law enforcement, vulnerability of societal institutions to electronic attack, export regulations and international competitiveness, and development of secure information systems.

Some programming may be required. After CPSC 202 and 223.

2 Course Description

This course is about cryptography and its applications to information and computer security. Privacy and security are central to our emerging "information society", and cryptography is a key technology for achieving them. It is also a fascinating field of study in its own right.

Information security, broadly defined, involves managing the collection, storage, and use of information. It includes issues of confidentiality, data integrity, availability, authenticity, and authority. Confidentiality refers to preventing information flow to unintended recipients. Data integrity ensures that information is correct and undamaged. Availability provides for information to be usable when needed. Authenticity identifies information with a source. Authority describes what actions are permitted by whom. Because of the ease with which information can be copied and transmitted, traditional physical means of control are of limited efficacy. Cryptography gives a way to build logical controls on the flow of information that are largely independent of the physical properties of the devices used to transmit and store information.

Information and computer security are broad fields that go way beyond what will be covered in this course. Privacy and information security are not simply technical problems but involve the legal, political, and social frameworks in which we live. Computer security includes topics such as physical security, access restrictions, activity monitoring, and control of software defects. While some of these topics will be mentioned in passing, the focus of this course is to understand the uses and limitations of the cryptographic tools that have application to privacy and security.

3 Tentative Schedule

The course comprises five modules, with time allocated roughly as follows:

- Security Properties (2 lectures)
- Classical Cryptography (7 lectures)
- Public Key Cryptography (5 lectures)
- Cryptographic protocols: hashing, authentication, secret spliting, pseudorandom number generation, bit commitment, secure multiparty computation (8 lectures)
- Real-World Applications: Voting, digital currency, anonymity (3 lectures)

Midterm Exam Wednesday, October 11, at the regular class time and room.

Final Exam Saturday, December 16, 7:00 pm, in a room to be announced.

These exam dates are firm, so you should avoid making other commitments on those days.

4 Course materials

Course Websites: This class will use two websites:

- Canvas: `https://yale.instructure.com/courses/29856`
- Zoo website: `http://zoo.cs.yale.edu/classes/cs467/2017f/index.html`

Canvas will be used for homework assignments and submissions, grading feedback, and emailed announcements. The Zoo website will be used for the syllabus, handouts, lecture notes, general announcements, and other course-related materials.

Textbooks: While no textbooks are required, the two books below are strongly recommended. Both are both available at Yale as licensed e-books. This means you can read them online or download PDF's and use them for free. Both are nice introductions to cryptography, and you will see that there is considerable overlap between the two. The first tends to be a little more focused on cryptographic theory and the second a bit more applied, but both are well written and useful for the material they cover.

- Christof Paar and Jan Pelzl, *Understanding Cryptography*, Springer, 2010, ISBN-13: 978–3–642–04100–6, ISBN-10: 364204100. Available at Yale as a licensed online book.
- Kościelny, Czesław, Kurkowski, Mirosław, Srebrny, Marian, *Modern Cryptography Primer*, Springer, 2013, ISBN 978–3–642–41386–5. Available at Yale as a licensed online book.

Additional references can be found on the course website under Resources.

5 Course Mechanics

Prerequisites: This course will be taught at an advanced undergraduate/graduate level and assumes a familiarity with basic concepts of mathematics and computer programming such as are covered in the official prerequisite courses, CPSC 202a and CPSC 223b. Graduate students should have an equivalent background. Some C/C++ programming will be required.

Requirements: Course requirements include written problem sets and programming assignments ($\sim$40%), a midterm exam ($\sim$20%), and a final exam ($\sim$40%). The approximate weights of each in determining the course grade are subject to change depending on the number and difficulty of the assignments actually given. Graduate students taking the course will be expected to perform at a higher level than undergraduates and may be required to do additional work.

Assignments and other announcements: Written problem sets and programming assignments will be posted from time to time on the handouts page of the Zoo website and will be announced on Canvas. Other course announcements will be posted on the Zoo website home page. It is your responsibility to check these pages frequently.

Help with Technical Material: The teaching assistant, Arseniy (Senia) Sheydvasser, will be holding scheduled office hours during the term. Times will be posted on the Zoo website. You are encouraged to meet with him with questions about the lectures, textbook, and problem sets. You may also send questions to him by email.

Other Questions: All questions about assessment and grading should be taken first to the TA. If she is unable to resolve your questions to your satisfaction, or if you wish to talk to me privately about any matter, you are always welcome to contact me, either by email or in person. Email is the preferred way to arrange an appointment with me.

6 Policies

Late Policy: Assignments will be due at 11:59 pm on the night of the stated due date. Late work will generally be subject to a penalty of 5% per day late unless accompanied by a Dean's excuse. A 2-hour grace period following the original due date will be granted during which no late penalty will be assessed. However, there will be no grace period in counting the number of days late for assignments turned in after the grace period. Work more than 4 days late will not be accepted, but alternative means for making up missed work may be arranged on an individual basis with a Dean's excuse.

Please contact the instructor or TA as soon as you know that you will be unable to submit work on time or to attend a scheduled exam so that suitable makeup arrangements can be made.

Policy on Working Together: This course follows the Yale College Undergraduate Regulations and the Yale Graduate School Professional Ethics and Regulations policies regarding cheating, plagiarism, and documentation, with which you should familiarize yourself. Briefly, if you use someone else's work, you must acknowledge it. If it's a piece of code, place the acknowledgment in your source file and explain clearly what parts are not your own. Similarly, if it's in a paper, the acknowledgment belongs in the paper itself. All work not so acknowledged must be your own.

You may of course discuss the lectures and readings with your classmates in order to improve your understanding of the subject matter. Helping each other learn to use the tools in the Zoo is also okay. However, the design and implementation of all programs and all submitted work must be your own except where other sources are explicitly noted.

You must never let another student see your work, either before or after the due date of the assignment. Sometimes you may be tempted to "help" your friends by letting them see your solution. Don't! This doesn't help them. To the contrary, it allows them to avoid the hard work of learning the material and deprives them of the educational experience they came to Yale to get.

You are always free (and encouraged) to come in and ask the TA or instructor for help about anything concerning the course. Please talk to the instructor if you have any questions about this policy.

Avoiding Plagiarism: You may neither copy from another student nor permit your own work to be copied, unless explicit permission is given for such collaborations. If your work is found in the possession of another student, you and the other student are equally guilty of plagiarism. To avoid unintended involvement in plagiarism, *your work should never be in the possession of another student*. Do not ask someone else to deliver or pick up your work. Do not let another student "borrow" your code to compare with theirs. Keep your files protected so that others cannot read them and carefully guard your password. Do not leave printed work in public areas such as the Zoo or in accessible wastebaskets. If you think your password may have been compromised, you must change it immediately and notify the instructor.

Policy on Computer Problems: The Yale College policy on "Use of Computers and Postponement of Work" in the Yale College Programs of Study, Academic Regulations, applies to this course. It is reproduced below.

> "Problems that may arise from the use of computers, software, and printers normally are not considered legitimate reasons for the postponement of work. A student who uses computers is responsible for operating them properly and completing work on time. (It is expected that a student will exercise reasonable prudence to safeguard materials, including backing up data in multiple locations and at frequent intervals and making duplicate copies of work files.) Any computer work should be completed well in advance of the deadline in order to avoid last-minute technical problems as well as delays caused by heavy demand on shared computer resources in Yale College."

Particularly relevant for this course are the cautions against leaving a programming assignment to the last minute when machines might be busy, printers broken, and so forth, and about safeguarding your data.

Policy on Technology in the Classroom: Cell phones are not to be used in class. Tablets and laptops are allowed only for course-related activities such as note-taking, reading slides and other materials from the course website, and quick internet searches on topics relevant to the lecture. Their use must limited so as to not distract you from paying attention in class. If in doubt, ask the instructor or TA first. Games, instant-messaging, reading email, and other diversions are not permitted. You may be asked to leave the class if these rules are not followed.

7 Computing Facilities

The Zoo: This course will use the Computer Science Department's educational computing facility, affectionately known as the Zoo. This facility contains modern workstations running Redhat Enterprise Linux 7. You will need to use these machines to prepare coursework. Look at

```
http://zoo.cs.yale.edu/help/
```

for information on getting started if you are new to the Zoo.

These days, most of you have your own laptops and may be wondering why you should be bothered with using a new computer system. The answer is because code development software is still not completely compatible across multiple platforms. If it works on your Mac or Windows PC but fails when the graders run it on the Zoo, you will lose points. If you ask for help with compiler errors on your personal machine, we might not be in a position to answer your questions. In short, develop your code on the Zoo! Regardless of where the code is developed, *your assignments will be*

graded according to how well they work on the Zoo. Assignments must be submitted electronically. Any handwritten materials should be scanned to a PDF file and the file submitted. Email subissions will not be accepted.

The Zoo machines support remote access via the SSH and VNC protocols, and also via the FastX software. These enable you to do your work remotely when it is inconvenient to go in person to the Zoo. Instructions on how to configure your machine for remote access will be posted to the course web site.

Course directory: The shared course directory, `/c/cs467`, is located on the Zoo server. You can access it from your Zoo course account. It will contain any software needed for this course and miscellaneous documentation and files. Public files there can be accessed via the web as well as from a Zoo node.