# Syllabus (Spring 2019)

## 1 Official Yale course listing

CPSC 367 01 (23226) Spring 2019
**Cryptography and Security** Final exam HTBA
Michael Fischer
TTH 2:30pm–3:45pm in AKW 200

An introduction to cryptography and information security. Cryptographic algorithms and their application to security of digital data are presented. Some topics include classical, symmetric, and public key cryptography; digital signatures; cryptographic hash functions; and pseudorandom number generation. Multiparty protocols such as zero-knowledge proofs, secret sharing, anonymous communication, and secure multiparty function evaluation are introduced. Practical applications of cryptography to secure network communication, secure password authentication, and blockchains are also covered. The emphasis is on cryptographic algorithms and protocols that can be useful in providing information security. Students interested in a more mathematical and rigorous approach to these topics should take CPSC 467 instead, or in addition to this course. This course may not be taken for credit after CPSC 467.

*Prerequisites:* Some programming 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:

- Security Properties
- Classical Cryptography
- Public Key Cryptography
- Cryptographic protocols: hashing, authentication, secret spliting, pseudorandom number generation, bit commitment, secure multiparty computation
- Real-World Applications: Voting, blockchain, SSL/TLS, Kerberos

**Midterm Exam** Tuesday, February 26, at the regular class time and room.

**Final Exam** HTBA.

## 4 Course materials

**Course Websites:** This class will use two websites:

- Canvas: `https://yale.instructure.com/courses/44181`
- Zoo website: `http://zoo.cs.yale.edu/classes/cs367/2019s/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.

**Online Resources:** Technical material on cryptography will be available in lecture notes and supplemented by several Yale-licensed e-books. This means you can read them online or download PDF's and use them for free. The first two are nice introductions to cryptography, and you will see that there is considerable overlap between the two. The first tends to be more focused on basic cryptographic theory and the second is a bit more applied, but both are well written and useful for the material they cover.

The von zur Gathin book contains a wealth of material from the basics to fairly advanced. It is a good reference for filling in gaps in the lectures. It also contains fascinating historical material in the lettered chapters that are intermixed with the modern technical material!

- 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.
- Joachim von zur Gathen, CryptoSchool, Springer, 2015, Online ISBN 978–3–662–48425-8. Available at Yale as a licensed online book.

**Additional references:** Additional references can be found on the course website under Resources. It will be updated from time to time during the term.

## 5 Course Mechanics

**Prerequisites:** This course will be taught at an intermediate undergraduate level. It assumes a familiarity with basic concepts of mathematics and computer programming such as are covered in CPSC 202 and CPSC 223. Some C/C++ programming will be required.

**Requirements:** Course requirements include written homework and papers, problem sets and programming assignments, class engagement, a midterm exam, and a final exam. The weights of each in determining the course grade will depend on the number and difficulty of the assignments actually given.

**Assignments and other announcements:** Written 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 the Course:** The teaching fellow (TF) for this course is Jaspal Singh. He will be holding scheduled office hours during the term. Times will be announced on Canvas and on the Zoo website. He can also be reached by email. You are encouraged to contact him with questions about the grading, lectures, textbook, and problem sets.

I am also happy to offer help by email or in person. Email is the preferred way to arrange an in-person 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 TF 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 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. Texting, games, instant-messaging, 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 Fedora 28 Linux. You will need to use these machines to prepare coursework. Look at

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

for information on getting started if you are new to the Zoo. A Zoo account will be automatically created for you if you don't already have one when you register as a shopper for this course.

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. If you lack needed software that has been installed on the Zoo for your use, you're on your own. 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*. Submission of assignments will be through Canvas.

The Zoo machines support remote access via the SSH and VNC protocols. These enable you to do your work remotely when it is inconvenient to go in person to the Zoo.

**Course directory:** The shared course directory, `/c/cs367`, 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 also be accessed via the web.