General Information
CSC 214P, “Cryptography”
Department of Computer Science
Grinnell College
August 29, 2019

Modern cryptography is a branch of applied mathematics. It is built on formal definitions, precisely stated assumptions, and rigorous proofs of the security properties of cryptographic systems. In this course, we’ll develop the basic principles of the subject and apply them to “perfect” systems such as the one-time pad and to some private-key symmetric systems with wider real-world applications.

The class meets in Noyce 3818 from 2 to 3:50 p.m. on Thursdays, beginning on Thursday, August 29.

Course Web site
https://unity.homelinux.net/courses/cryptography/

The Textbook

Jonathan Katz’s page at the Maryland Cybersecurity Center
https://www.cyber.umd.edu/faculty/katz/

Yehuda Lindell’s page at Bar-Ilan University
https://u.cs.biu.ac.il/~lindell/

Introduction to Modern Cryptography
https://www.cs.umd.edu/~jkatz/imc.html


The Instructor
The instructor for this course is John David Stone. My office is Noyce 3829, near the east end of the long corridor on the third floor of the Noyce Science Center, on the north side (facing Eighth Avenue).

My office hours for fall 2019 are Mondays, from 2 to 4 p.m.; Tuesdays, from 10 a.m. to noon; Thursdays, from 9 to 11 a.m.; or by appointment.

I can be reached by e-mail as reseda@unity.homelinux.net or by telephone at (641) 269–3181.

I recommend the use of encryption to protect the contents of e-mails in transit. If you haven’t yet started encrypting your e-mail, you might consult the Electronic Frontier Foundation’s “Surveillance Self-Defense” Web site for advice and instructions. The EFF recommends the use of an encryption system called “Pretty Good Privacy” (PGP):

“How to: Use PGP for Linux”
https:ssd.eff.org/en/module/how-use-pgp-linux

“How to: Use PGP for macOS”
https:ssd.eff.org/en/module/how-use-pgp-mac-os-x

“How to: Use PGP for Windows”
https:ssd.eff.org/en/module/how-use-pgp-windows
A PGP encryption key that you can use to send messages to me is available on the Web:

- PGP public key for reseda@unity.homelinux.net
  https://unity.homelinux.net/reseda-public-key.txt
- MIT public-key server (a database of PGP users’ public keys)
  https://pgp.mit.edu/

To confirm that the key you download really is my public key, use your PGP software to extract and examine its “fingerprint.” If the result is

   EA7D 19D0 1A17 28D8 8F88 F745 6BC0 36C6 CDFD A8C2

then the key you have obtained is the right one to use.

Class Attendance

I expect you to attend every session of the class and to participate actively. It is especially helpful if you raise for discussion any questions you may have about the day’s topic, the assigned reading, or the exercises. I suggest that you write out such questions as part of your preparation for class sessions and pose them as opportunities arise.

Notwithstanding that general expectation, class attendance is optional. However, if you miss a class session for any reason, I will assign one or more makeup exercises for that session. Your absence is automatically excused when you have submitted solutions for those exercises.

Days of Religious Observance

Grinnell College acknowledges and accommodates the religious diversity of its students, faculty, and staff. If you miss a class session in order to fulfill a religious obligation, the accommodation is the one described in the preceding section: Your absence is excused once you have submitted solutions for the makeup exercises.

In religious matters, I am a free thinker. I have no religious obligations that are tied to specific days, and I expect to attend all of the class sessions scheduled for this semester.

Requirements

Each student in the course is expected to read the textbook and handouts carefully, to learn the ideas, methods, and techniques presented there, to submit solutions to exercises requiring the application of those ideas, methods, and techniques, to prepare for and attend the sessions of the class, and to participate in the discussions, labs, and in-class exercises conducted during class sessions.

Readings. In the schedule of topics for the course, I have generally specified reading assignments between successive class meetings. Please study each such reading before the beginning of the class that follows it in the schedule.

Exercises. Some of the assigned exercises for this course will be development exercises, while other will be demonstration exercises.

Development exercises are occasions for experimentation and learning. In preparing solutions to development exercises, you may exchange ideas and implementations with one another and, if you prefer, prepare and submit group solutions. You may also research the exercises online, in libraries, or in conversation with others outside the class, and you may incorporate, adapt, and improve any relevant material that you discover to produce your own solutions, provided that you credit your sources properly and cite them correctly.

We will often discuss development exercises in class and in mentoring sessions. During those discussions, you may ask questions about those exercises and incorporate what you learn into your solutions (again, with proper credit and correct citation).
In some cases, I’ll ask you to revise and resubmit your solutions to development exercises after you have had a chance to read and reflect on my comments. Ideally, you will be able to assemble the products of your work on these exercises into a portfolio of solutions that you can share with others who may be interested, such as graduate school admission committees, potential employers, and perhaps your friends and family members. So we’ll take some extra care to make them look good.

Demonstration exercises, on the other hand, are opportunities for you as an individual to demonstrate what you have learned. Collaboration on demonstration exercises is not permitted, even with appropriate citation. In evaluating your solutions these exercises, I will assume that they are exclusively your own work.

**Class sessions.** Most of the class sessions will consist mainly of asking and answering questions about the readings and exercises. I usually address students directly instead of waiting for volunteers, so you should expect to ask and answer questions on demand and prepare accordingly.

**Grading**

Section IV.A.4 of the Faculty Handbook explains the duty of faculty members to report grades as follows:

> Among the accepted responsibilities and obligations of each member of the faculty is that of reporting to the Registrar, at the appointed times, grades in accordance with the grading system and with the grading regulations which the faculty shall from time to time adopt. Further, faculty members are expected to make timely evaluations of students throughout the year.

> Inherent in the responsibility of reporting grades is the further understanding that all such grades reported shall have been determined, in the final analysis, on the basis of the faculty members own professional evaluation of each individual students work.

> This above indicated responsibility is considered to be part of the contractual relationship between the individual faculty member and the College, and the failure to fulfill this obligation will be considered a breach of contract.

In each of my courses, I fulfill this responsibility to the letter. However, I advise students that they should not regard the grades reported to the registrar as complete or even adequate assessments of their intellectual strengths and weaknesses. Grinnell College’s grading system is extremely inexpressive and vague. I urge you to pay much closer attention to your verbal interactions with me and to the comments that I make on your course work than to the grade that I report at the end of the course. Nonetheless, that grade is, as specified, based entirely on my professional evaluation of your individual work.

Specifically, your grade will be based on your contributions to class sessions (roughly 40%) and your performance on demonstration exercises (roughly 60%).

**Copyrights and Licensing**

Source code that I create for this course and make available on MathLAN or at the course Web site is licensed under the GNU General Public License (unless otherwise indicated in the source-code file itself). Code released under the GPL can be copied, studied, revised, improved, and redistributed freely, provided that all copies and derived programs are released under the same license and correctly attributed.

Similarly, handouts and other prose course materials that I have created and distributed on MathLAN, at the course Web site, or in hard copy are licensed under the Creative Commons Attribution–ShareAlike 4.0 International License and can be copied, studied, revised, improved, and redistributed freely, provided that my authorship of the original work is acknowledged and that any copies or derived works are released under the same license.
Under Grinnell College’s copyright policy, a student who submits a program or a prose text to satisfy a requirement of this course retains the copyright to it. Similarly, a group that submits such a work has and retains a collective copyright. In either case, however, the College asserts the right to distribute the work within the College community for instructional or administrative purposes without paying any royalty to the student.

You may, of course, choose to publish your work under some more generous license, and I encourage you to use the GNU General Public License (version 3) for software and the Creative Commons Attribution–ShareAlike 4.0 International License for prose.

“GNU General Public License”
https://www.gnu.org/licenses/gpl-3.0.en.html

“Attribution-ShareAlike 4.0 International (CC BY-SA 4.0)”
https://creativecommons.org/licenses/by-sa/4.0/deed.en_US

“Grinnell College Copyright Policy”
https://www.grinnell.edu/sites/default/files/documents/copyright_0.pdf

To my knowledge, the College has never abused its claimed right of distribution or used it in a way that would be contrary to the interests of student authors. Since 2013, however, the College has designated a large number of third parties as school officials with a “legitimate educational interest” in student records. For example, the Registrar has designated Microsoft Corporation, which manages the College’s e-mail and provides some cloud-based services to the College community, as a school official, entitled to access a great many notionally private files and e-mail messages created by students and faculty. Unfortunately, Microsoft has an extremely sketchy corporate track record that includes many instances of exploitation of its customers and users. Its rap sheet includes a felony conviction in American criminal courts on charges of abuse of monopoly and a similar conviction in the European Union. In addition, since 2007, Microsoft has routinely given the National Security Agency access to most of its users’ emails, video chats, and cloud document storage.

In my opinion, Microsoft cannot be trusted to respect the rights and interests of student authors. Accordingly, I now advise students not to store any original writing, including source code for computer programs, on the College’s cloud-based storage servers and not to e-mail it (without encryption) to or from any @grinnell.edu address, since any of those acts might be construed as allowing such so-called “school officials” to read, copy, modify, distribute, and mine data from your original work without your permission.

Collaboration and Plagiarism

Since you will receive credit as an individual on the basis of your performance in this course, it would be unethical to submit a solution to any of the demonstration exercises that is not entirely your own work. To borrow other people’s solutions without acknowledgement is improper in any case; but on demonstration exercises it is also improper to take answers or partial answers from others, even if their contributions are explicitly acknowledged.

If I encounter clear indications of plagiarism or academic dishonesty, the Committee on Academic Standing will deal with them. The College’s policies for faculty members prohibit me from trying to investigate major offenses on my own. For the same reason, I impose penalties for academic dishonesty only as directed by the Committee on Academic Standing.

Because in recent years the Department of Computer Science has received mixed signals from the Committee on Academic Standing and from the Office of the Dean about the nature and scope of academic dishonesty, we have formulated departmental standards of academic integrity for students in our courses. They are available on line: