

CIS 400/628: Introduction to Cryptography

Spring 2005

Syllabus

Tuesday, Thursday 1230–1350, 1-019 CST

Instructor: Steve Chapin
e-mail: chapin@ecs.syr.edu
Office: 3-125 CST, 443-4457
Office Hours: Tuesday 1500-1600, Wednesday 1000–1100
additional times by appointment

TA: Kanat bolazar
e-mail: kanat2@yahoo.com
Office:
Phone:
Office Hours: TBD

Purpose

This is a mixed undergraduate and graduate course in the basics of cryptography. It covers encryption, basic cryptanalysis, public and secret key encryption, block ciphers, digital signatures, zero-knowledge proofs, elliptic curve cryptography, and quantum computing.

Text

There are three primary texts for this course; You should own at least one of them.

1. Wade Trappe and Lawrence C. Washington, *Intro. to Cryptography with Coding Theory*, Prentice-Hall, 2001, ISBN 0130618144.
2. Robert Lewand, *Cryptological Mathematics*, MAA, 2000, ISBN 0883857197.
3. Paul Garrett, *Making, Breaking Codes: an Introduction to Cryptology*, Prentice-Hall, 2001, ISBN 0-13-030369-0.

The following are recommended for additional references:

1. Niels Ferguson and Bruce Schneier, *Applied Cryptography*, ISBN 0-471-22357-3, John Wiley & Sons, 2003.
2. Bruce Schneier, *Applied Cryptography*, 2nd edition, ISBN 0-471-11709-9, John Wiley & Sons, 1996.

3. Alfred J. Menezes, Paul C. van Oorschot, and Scott A. Vanstone, *Handbook of Applied Cryptography*, ISBN: 0-8493-8523-7, CRC Press, 2003. Available **free** online at <http://www.cacr.math.uwaterloo.ca/hac>.

Grading Policy

The grade for this course will be assigned based on (all percentages are approximate):

1. Homework (both paper and programming) 30%
2. Quizzes 30%
3. Midterm project 20%
4. Final project 20%

Quizzes

There will be no exams in this course. There will be approximately 10 quizzes, and your lowest quiz grade will be dropped.

Homework and Programming Assignments

Homework will be of three types:

1. Mathematical paperwork, including proofs derivations of formulae.
2. Programming assignments, generally implementing cryptographic primitives.
3. Cryptographic puzzles and problems to solve.

There will approximately 10 homework sets over the duration of the course. They will be handed out on Thursdays and due the next Thursday that class meets. Your lowest homework grade will be dropped.

Midterm and Final projects

These will be substantial projects. Students may work singly or in pairs on these projects, although portions of each project must be individual efforts. Graduate students are expected to take on more challenging projects than the undergrads.

Late Policy

All assignments must be turned in by the due date. There will be no extensions for any assignment. However, each student will have 72 “free late hours” to spend throughout the semester. It is up to you when you use them. I encourage you not to spend them all early in the semester, as scheduling conflicts, disasters, etc. will likely arise later and you’ll want them then.

Honor Policy

Students are expected to do their own work. Unless explicitly given permission, you should not work with other students on the programming of your assignments. Discussion of concepts is fine, but your code should be your own. Code sharing is also a violation of this policy. Violation of this policy is grounds for failure from the course.

At times, you may be working in teams for this course, and of course may share code and ideas within a single team, but unless explicitly given permission, you should not work with other teams on your assignments.

The essence of our honor policy is taken from the University of Virginia honor policy, and can be stated as, “Students will neither give nor receive aid on assignments.” At the beginning of the course, students are required to submit a signed, dated statement saying, “I have read, understand, and agree to abide by the honor policy for CIS 400/628.”

In addition, on each individual assignment or quiz, students must write the statement, “I have neither given nor received aid on this {assignment, quiz, project}.” For team assignments and projects, students must write the statement, “With the exception of my partner, I have neither given nor received aid on this {assignment, project}.” This statement must be dated and signed.

Violations of the honor policy are grounds for failure from the course.

Dr. Royer, who has taught this course in the past, has an excellent discussion on “Avoiding Problems” on his course web page¹ which I will now quote (quoted material in sans serif font):

1. Read the following two webpages on plagiarism. They are very clear and give nice examples.
 - “Plagiarism: What It is and How to Recognize and Avoid It” from Indiana University’s Writing Tutorial Service.²
 - “What Is Plagiarism?” from Georgetown University.³
2. Always give credit when credit is due. For example, suppose you discuss homework problem 5 with Joe Hacker. Then to be in the clear you should include the statement to [sic] your homework paper
I discussed this problem with Joe Hacker.
and make what you turn in is your work, not Joe’s.
3. When in doubt about a situation, ask me.

Note that this is an example of citing Dr. Royer’s intellectual property (and it’s recursive, as he cites others’ as he uses it). Please note that you should ask *me*, not Dr. Royer, if you have a question about the honor policy for the course this semester.

¹<http://www.cis.syr.edu/royer/crypto/admin.html>

²<http://www.indiana.edu/wts/pamphlets.shtml>

³<http://www.indiana.edu/wts/pamphlets.shtml>

Class Notes

I will make my notes available on-line. My current web page for this course is

<http://www.hpdc.syr.edu/~chapin/cis628>.

This does not relieve you of the responsibility of reading relevant material or knowing its contents. While I will make a good-faith effort to have the notes available before class, you should not rely on this as a substitute for paying attention and taking notes. I give you these notes to relieve you of the drudgery of making them and to free your minds to concentrate in class.

Mailing Lists

We maintain two class mailing lists; one for questions from students to the TAs and professor, and one for information and answers flowing from the TAs and professor to the students. The first mailing list is `crypto_ta@hpdc.syr.edu`, and the second you don't need to know.

Course Topics

This course will cover the following topics, at a minimum. Additional lectures and topics will be inserted as time permits.

- Introductory lecture. Presentation of syllabus and history and background of cryptography. Introduction of terms and fundamental mathematics.
- Monoalphabetic ciphers.
- Polyalphabetic ciphers.
- Polygraphic ciphers.
- Secret key ciphers and block ciphers (DES).
- Public Key Cryptography; RSA & AES.
- Signatures.
- Key agreement.
- Protocol Design.
- Quantum Cryptography/Computing.
- Games.
- Zero-knowledge protocols.