

Cryptology and Coding Theory
Course Info Sheet
Fall 2006

Meeting Times/Location: **M, TH** 4:00-5:50
Academic Center 328 (Olin College)

Instructor Information:

Professor Sarah Spence Adams

Office: Olin Center 258, Olin College

Office Phone: 781.292.2536

Email: sarah.adams@olin.edu

Office Hours: Mon/Th 3-4pm (Olin's AC328), Weds 1:30-3:00 (Olin Center 258) and by appt.

Professor Gordon Prichett

Office: Babson Hall 212A, Babson College

Office Phone: 781.239.4428

E-mail: prichett@babson.edu

Office Hours: Tues, Weds 3-5pm (Babson Hall 212A) and by appt.

Course Assistant/Grader: TBA

This course will introduce you to the exciting fields of cryptology and coding theory. Cryptology combines the studies of cryptography, the creating of masked messages, and cryptanalysis, the unraveling of masked messages. Coding theory is the study of coding schemes used to detect and correct errors that occur during the data transmission. To study these symbiotic disciplines, you will learn some basic linear algebra, abstract algebra, number theory, probability, and combinatorics. You will also develop skills in problem solving, clear thinking, logical reasoning, and working in groups. We hope that you find this course to be both challenging and fun – you will walk away with technical proficiency in fields crucial to information exchange today, improved skills relevant to life-long learning, and hopefully a whetted appetite to pursue additional mathematics/technical courses.

Learning Objectives/Measurable Outcomes

By the end of this course, students should be able to:

- Understand the goals and trade-offs associated with encryption and error-control coding systems.
- Individually solve and communicate the solutions to problems fundamental to the studies of cryptology and coding theory. Topics include:
 - Historical ciphers, cryptanalysis of basic ciphers, RSA and other modern public-key cryptosystems, relevant introductory probability, number theory, and abstract algebra.
 - Check digit schemes, linear codes, cyclic codes, relevant introductory probability, linear algebra, and abstract algebra.
- Work with a small group to solve and communicate the solutions to problems fundamental to the studies of cryptology and coding theory.
- Self-direct a group project on a specialized topic in cryptology or coding theory.

Competencies Assessed:

- **Quantitative Analysis** (Analyze and mathematically solve a variety of problems.)
- **Communication** (Develop technical writing skills through written project report and through writing solutions on homework and tests; Develop oral communication skills through oral project report and through giving oral explanations of problems, solutions, and concepts.)

Additional Competencies Developed/Utilized:

- **Teamwork** (You will do a significant amount of problem solving in groups-your teamwork skills should improve throughout the semester)
- **Life-long learning** (Develop perseverance and skills for effective self-motivated and self-monitored work.)
- **Qualitative Analysis** (Develop understanding and ability to explain the mathematical concepts and basic implementation issues involved with cryptology and error-control coding.)
- **Understanding of Context** (Learn about social and cultural implications of the technologies studied.)

Texts:

- *Introduction to Cryptography with Coding Theory* by Trappe and Washington, 2nd edition, Prentice Hall, 2006.
- *The Code Book* by Simon Singh, Doubleday, 1999
- *Introduction to Algebraic Coding Theory with Gap*, Sarah Spence Adams, 2005. (Available freely online.)

Attendance:

Class meetings will vary from day to day. Sometimes, we will cover material in your texts but offer different examples or applications. Sometimes we will cover material not covered in your texts. Sometimes you will be giving presentations. Often you will be working problems. Sometimes you will be taking quizzes or tests. We expect you to be there to participate and engage in conversation with your peers and us. If you do miss a class, please seek out one of your peers to find out what you missed, including any announcements.

Homework:

- **Reading:** Each class will have associated reading assignments, which helps broaden and deepen your understanding of the material. Usually, you will be asked to do the reading before class.
- **Practice Questions:** These questions will help focus your reading, self-check your comprehension of the material, and prepare you for the group homework, quizzes, and tests. You should try these problems on your own first, and then collaborate with classmates to ensure your understanding.
- **Homework Sets:** You will be assigned approximately five homework sets throughout the semester. These homework sets will be completed in **pre-determined groups**, and each member of the group will receive the same grade. You are encouraged to solve these problems only with your team-mates. Any collaboration with students outside your group must be cited.

Using Resources on Homework:

It is **strictly forbidden** to use any sources of solutions to any problems (from other schools, on the web, etc.).

Other sources of help (e.g. library books, the TA, your professors) are permitted under the following two conditions:

- You must never simply copy a solution (from a book or a friend) or hand in a solution that you do not fully understand. By handing in a solution, you are certifying that you understand it completely and you can independently solve similar problems.
- You must **always cite** your source of help to each problem. Simple notes in the margin such as “checked answers with Luisa,” “used back of book,” “used book A by author B,” “helped by TA” are perfectly fine. Feel free to use abbreviations—we don’t want citing to be a time burden. Getting in the habit of always citing sources of help is good professional practice and is in the spirit of learning and the Honor Code.

If you do not use any sources or receive any help from friends, then please write “No Help” on the top of your paper.

If you have any questions about what resources are allowed or how to cite them, please just ask!

Other Requirements HW:

It is essential that all turned in homework be neatly written or typed. On the upper right hand corner of the first page, please list your full name(s), Cryptology and Coding Theory, the assignment (e.g. “Homework Set #1”) and the due date for the assignment. You must staple all pages together. Each problem must be clearly labeled and final answers (if applicable) should be circled. You must show your work, which means that steps must be clearly explained. Unless you are asked to submit your work electronically, your work should be done on standard sized (8.5” by 11” paper) with clean edges and few erasures. Neatness and clarity of explanation are essential; your exposition will be evaluated.

Late homework is not accepted unless there is a real emergency. Please do not ask for an exception.

Quizzes:

To check comprehension and prepare you for the exams, we will give approximately three quizzes.

Project:

In a small group, you will choose and investigate a cryptology or coding theory topic not covered in class. Your group will deliver an in-class presentation and write a paper on your topic of choice. You will assess your classmates’ projects.

Tests:

You will have two in-class tests, tentatively scheduled on October 10 and November 13.

Grading:

Participation/Engagement: 5%

Quizzes: 10%

Homework/Project: 25%

Test 1: 30%

Test 2: 30%

Office Hours:

Please come to office hours with questions big and small! Maybe you don't even know what your questions are: we can probably still help. Sometimes a few minutes in office hours can make a big difference. If you need a special appointment, please ask.

Supplies:

We recommend you use a loose-leaf notebook. This way, you can keep your class notes, various homework problems, various handouts, etc, all in order. Please save all of your work until (at least) the end of the semester.

Syllabus:

The daily schedule is subject to change as we go. All assignments are subject to change.

Special Needs:

Any student who is entitled to an academic accommodation based on the impact of a documented disability should contact one of the professors to discuss her or his specific needs. To coordinate reasonable accommodations, Babson students should additionally contact Erin Evans, Coordinator of Disability Services at 781-239-4075 or in Hollister Hall; Olin students should additionally contact the Office of Student Life (x2325); and Wellesley students should additionally contact Barb Burck at the PLTC (x2641, 3rd floor Clapp Library).

Honor Code:

We regard the Honor Code of each of your colleges as essential to academic integrity. Please express any concerns in a timely fashion.