Math/CS 124 — Codes and Encryption

Time and place: 10:05–11:55am, TTh, Adams 217

Professor: David J. Hunter, Ph.D.

e-mail:	`dhunter@westmont.edu`
Office Phone:	x6075
Office:	Winter Hall 303
Student Hours:	M–Th 3:30–5:00pm, or by appointment.

Catalog Description: (Four credit hours) Prerequisites: MA/CS-015 or MA-020. Modern applications of computing demand that the storage and transmission of data be secure and reliable. Cryptography is the study of techniques for protecting data from adversaries, while coding theory deals with representing data robustly in digital form. This course provides an introduction to these related fields. Topics include basic number theory and modern algebra, classical and modern cryptosystems, discrete logarithms, hash functions, digital signatures, elliptic curves, and error-correcting codes.

Prerequisites: MA-015 and/or MA-020. Programming experience is desirable but not essential.

Overview: This course will give a general introduction to cryptography and coding theory. The point of view will be mathematical, yet applied. We will focus on the general mathematical principles that govern the ways that information is stored and transmitted securely. We will not dwell too heavily on the technicalities of specific protocols and implementations. Rather, we strive to understand the concepts that underlie the technology, so that you will be prepared to view current and future implementations as scientists and engineers, not as technicians.

Textbook: *Introduction to Cryptography with Coding Theory*, by Trappe and Washington, 2nd Edition. If you have your own computer, install R and RStudio on it (`https://www.rstudio.com`).

Grading: Grades are weighted as follows.

Written Assignments:	25%
R Course Package:	25%
Midterms:	2 @ 15% each
Final Exam:	20%

The final exam will be on Wednesday, December 16, from 8:00–10:00am. Finals will not be rescheduled to accommodate travel arrangements.

You should expect a written assignment due the night before every class meeting. You will submit them on Canvas (`https://westmont.instructure.com`) as PDFs, which you can create by scanning your written work using a scanning app. If you prefer, you can typeset these assignments using LaTeX or a word processor.

Over the course of the semester, you will develop an R package containing a library of functions for solving problems in cryptography and coding theory. Typically, I will give you a template including function prototypes, ROxygen comments, and test cases that your functions should satisfy. You will submit successive versions of this package as `tar.gz` files on Canvas.

Attendance: Please show up to class on time; it is rude and distracting to your classmates if you come to class late. Significant tardies count as absences. If you miss an excessive number of classes, you will almost definitely do poorly in this class. I consider it excessive to miss more than two classes during the course of the semester. If you miss more than four classes without a valid excuse, I reserve the right to terminate you from the course with a grade of F. Work missed (including tests) without a valid excuse will receive a zero.

Other Policies: Learning communities function best when students have academic integrity. Cheating is primarily an offense against your classmates because it undermines our learning community. Therefore, dishonesty of any kind may result in loss of credit for the work involved and the filing of a report with the Provost's Office. Major or repeated infractions may result in dismissal from the course with a grade of F. Be familiar with the College's plagiarism policy, found at: `https://www.westmont.edu/office-provost/academic-program/academic-integrity-policy`.

In particular, providing someone, actively or passively, with an electronic copy of your work is a breach of the academic integrity policy. Do not email, post online, or otherwise disseminate any of the work that you do in this class. If you keep your work on a repository, make sure it is private. You may work with others on the assignments, but make sure that you type up your own answers yourself. You are on your honor that the work you hand in represents your own understanding.

Tentative Schedule: The following schedule is a rough first approximation of the topics in *Trappe* that we plan to cover; it is subject to revision at the instructor's discretion. Chapter 3 (Basic Number Theory) will be covered throughout the course when the relevant topics arise.

- Chapter 2: Classical Cryptosystems
- Chapters 4–5: DES and AES
- Chapter 6: The RSA Algorithm

  Midterm #1 (through Chapter 6)
- Chapter 7: Discrete Logarithms
- Chapter 8: Hash Functions
- Chapter 9: Digital Signatures
- Chapter 16: Elliptic Curves

  Midterm #2 (through Chapter 16)
- Chapter 18: Error Correcting Codes

  Final Exam (cumulative, with an emphasis on Chapter 18)

Program and Institutional Learning Outcomes: The mathematics and computer science department at Westmont College has formulated the following learning outcomes for all of its classes. (PLO's)

1. Core Knowledge: Students will demonstrate knowledge of the main concepts, skills, and facts of the discipline of mathematics.
2. Communication: Students will be able to communicate mathematical ideas following the standard conventions of writing or speaking in the discipline.
3. Creativity: Students will demonstrate the ability to formulate and make progress toward solving non-routine problems.
4. Christian Connection: Students will incorporate their mathematical skills and knowledge into their thinking about their vocations as followers of Christ.

In addition, the faculty of Westmont College have established common learning outcomes for all courses at the institution (ILO's). These outcomes are summarized as follows: (1) Christian Understanding, Practices, and Affections, (2) Global Awareness and Diversity, (3) Critical Thinking, (4) Quantitative Literacy, (5) Written Communication, (6) Oral Communication, and (7) Information Literacy.

Course Learning Outcomes: The above outcomes are reflected in the particular learning outcomes for this course. After taking this course, you should be able to:

- Demonstrate understanding of the theoretical basis for cryptography and coding theory. (PLO 1, ILOs 3,4)
- Write and evaluate mathematical arguments according to the standards of the discipline. (PLO 2, ILOs 3,5)
- Construct solutions to novel problems, demonstrating perseverance in the face of open-ended or partially-defined contexts. (PLO 3, ILO 3)
- Consider the ethical implications of the subject matter. (PLO 4, ILO 1)

These outcomes will be assessed by written assignments, programming assignments, and written exams, as described above.

Accommodations for Students with Disabilities: Students who have been diagnosed with a disability (learning, physical or psychological) are strongly encouraged to contact the Disability Services office as early as possible to discuss appropriate accommodations for this course. Formal accommodations will only be granted for students whose disabilities have been verified by the Disability Services office. These accommodations may be necessary to ensure your equal access to this course. Please contact Sheri Noble, Director of Disability Services (310A Voskuyl Library, 565-6186, `snoble@westmont.edu`) or visit `https://www.westmont.edu/disability-services` for more information.