Math 400: Senior Seminar
Cryptology
Occidental College Fall 2017

Jay Daigle

Course Goals

Cryptology is the study of sending secret messages over insecure communication channels. Cryptographic capabilities are important to politics and foreign affiars, and underly the functioning of a great deal of the modern economy. In this course we will study the mathematical theories and techniques that make cryptography function, and also those that break it. We will learn how these mathematical tools influence the use of cryptographic systems, and practice explaining these implications to people without developed mathematical backgrounds.

By the end of this course, you will

1. understand the mathematical underpinnings of cryptographic systems and be able to analyze their security.
2. see how a problem-centric approach brings many different ideas and fields of math together to solve problems.
3. practice communicating mathematical ideas in writing and in oral communication, and translating technical mathematical ideas for a lay audience.
4. relate your mathematical knowledge of cryptographic systems to newsworthy events and policy issues.

Instructor Info

Lectures:	R 3:05 – 4:30 PM	Mosher 3	
Instructor:	Jay Daigle	**Office Hours:**	MWF, 1:30 – 3:00 PM
Office:	Fowler 305	**Often in Office:**	MWF, 12:45 - 3:00 PM, 4:00 - 5:00 PM
Email:	gdaigle@oxy.edu		R, 1:30 - 3:00 PM, 4:30 - 5:00 PM
Course Webpage:	`http://jaydaigle.net/cryptology`		

References

There is no mandatory textbook for this course. I will post complete lecture notes and homework assignments on the course webpage. I will primarily be drawing on the following two sources:

- *An introduction to mathematical cryptography* by Jeffrey Hoffstein, Jill Pipher, and Joseph H. Silverman. This is available for free electronic access through the library.
- *Introduction to Cryptography with Coding Theory* by Wade Trappe and Lawrence C. Washington.

Grading

- **Homework: 65%**

  The bulk of your grade in this course will come from weekly assignments, due at the beginning of class each week. These assignments will feature a mix of mathematical problems and short writing prompts relating the math we have studied to real-world practical applications and concerns.

- **Presentation: 30%**

  You will each give one approximately 15 minute presentation on a cryptologic topic of your choice; I will provide a list of potential topics, but am also open to other topics of your suggestion.

  Your grade on the presentation will be allocated:

  - 10% for submitting notes and slides to me the Monday before your scheduled talk;
  - 10% for my evaluation of your talk, according to a rubric I will hand out;
  - 10% for the evaluation of your talk by your fellow students according to the same rubric.

  If you have a preference to give a talk earlier in the term, please let me know. I will grade the earlier presentations slightly more leniently than the later presentations.

- **Presentation feedback: 5%**

  I will ask you to evaluate the presentations of your classmates. Completely filled out evaluations will be worth full credit; incomplete evaluations will be worth half credit. This means you have to attend class to see and evalute the presentations! Please come talk to me if there is a class that you cannot attend for some reason and I should be able to accommodate you.

Schedule

Week	Topic	Field of math
Week 1	Intro to ciphers	Permutations and Modular Arithmetic
Week 2	Cryptanalysis and one-time pads	Models and Entropy
Week 3	DES and symmetric encryption	
Week 4	Diffie-Hellman and El-Gamal	Discrete Logarithm
Week 5	RSA	Factoring
Week 6	Digital Signatures	
Week 7	Elliptic Curves	Groups and Geometry
Week 8	TBA	
Week 9	TBA	
Week 10	Student presentations and bonus topic	
Week 11	Student presentations and bonus topic	
Week 12	Student presentations and bonus topic	
Week 13	Student presentations and bonus topic	

Other topics: Lattices, pseudorandom number generators, hashing, coding theory, collision attacks, computational complexity, entropy, unicity distance.

Course Policies

- **Homework**: There will be weekly homework assignments, due at the end of class each week. The homework will primarily consist of technical and mathematical content, but will touch on social impacts and communication ability. Homework is the primary way you will be graded in this course.

  I will *not* except late homework without prior permission or a note from the dean or the health center. If you need an extension, please email me before the homework is due. I am usually up late.

  Please begin the homework early, and discuss it with your classmates and with me. This is important enough to get its own paragraph.

- **Coding:** Many of the homework problems can be solved quickly via computer analysis. This is an important and legitimate skill, but only if you are doing it yourself and not simply borrowing someone else's solutions.

  Consequently, you are welcome to use any sort of computer tools on the homework, but you must write the code yourself and attach a copy of the code you use to the work you hand in. (I will not be grading the quality of your code; this is primarily to ensure that you aren't just downloading someone else's software and using it to do the homework for you).

  I am also aware that this course has a wide variety of knowledge of coding and comfort with computers. No particular computer or coding skills are a prerequisite for this course, and coding will not be required.

- **Final Presentation:** Each of you will give a fifteen-minute presentation on a cryptologic topic of your choice during the last four weeks of the course.

  The primary goal of this talk is to explain a mathematical idea to a non-mathematical audience, much as you would in a workplace. As such, your talk should explain the basic mathematical idea behind your topic (without going into technical details!) and then explain why your topic is useful and interesting and relevant. News hooks are not required here, but are helpful.

  I'll provide a more detailed prompt and rubric for this presentation as the term progresses.

- **Disabilities:** It is the policy of Occidental College to make reasonable accommodations for qualified individuals with disabilities. If you are a person with a disability and wish to request accommodations to complete your course requirements, please make an appointment with the course instructor as soon as possible to discuss your request. For information on documentation requirements, contact the Center for Academic Excellence (x2545).