APM5347 The Mathematics of Cryptology (4 credits)

From the OU catalog:

Introduction to the mathematics behind cryptology. It is suitable for advanced undergraduate or graduate students. The aim is to explain how encryption works (cryptography) and how one can sometimes break codes (cryptanalysis). It is suggested that students take CSE 681 Information Security before Mathematics of Cryptology.

> Encryption works. Properly implemented strong crypto systems are one of the few things that you can rely on. – Edward Snowden

Summary

Instructor:	Dr. Serge Kruk
Email:	kruk@oakland.edu
Office:	MSC 548
Office hours:	W 1300h-1500h
Textbook:	An Introduction to Mathematical Cryptography by Hoffstein, Pipher and Silverman
Additional material:	Keijo Ruohonen's course notes. (Unpublished. Used with permission) Modern Cryptanalysis by Swenson Algorithmic Cryptanalysis by Joux

Knowledge areas

From the ACM Computer Science Curriculum, this course covers the following knowledge areas:

- AL: Algorithms and complexity.
- CN: Computational science.
- DS: Discrete structures.

Material covered

- Simple ciphers and cryptanalysis based on counting.
- Refresher in number theory and algebra.
- Basic modern cryptography.
- Number theoretical ciphers and potential attacks.
- Block ciphers.
- Some basic algorithms generally useful.
- General cryptanalysis techniques.
- Linear cryptanalysis.
- Differential cryptanalysis.
- Lattices.

Learning outcomes

Students will be able to:

- Understand the number theory and algebra required for modern encryption.
- Deeply understand how the more common cryptography schemes work.
- Understand some of the cryptanalysis methods.
- Understand some of the basic algorithms used in cryptography.

Grading

- Homework: 20%
- Test 0: 20% Jan 17
- Test 1: 20% Feb 14
- Test 2: 20% Mar 21
- Final: 20% Apr 23

Corrections

After a test, I will often allow students to turn-in a corrected version of the test. The reason for this, contrary to students' belief, is that a test is a learning tool, not only an evaluation tool. A good correction may earn you back some of the points missed during the test, and will allow you to learn material that you failed to learn while preparing for the test. The rules for a test correction:

- You must do the corrections alone. No help of any kind. No discussion with peers. Find the answers in the book or in your notes.
- You must turn in a paper that states the questions, then answers them, in the order presented on the test.
- You must answer **all** questions, not only those you missed on the test. (While grading a test, I allow some slips because I understand the difficulty of answering under time constraints. Do not expect such munificence on a test correction.)
- Your answer must be written in English, be complete and be correct.
- Your corrections must be typed or written with impeccable penmanship. If your handwriting is bad, type your solutions.

Late Policy

Late homework assignments are **not** accepted. Missed tests or quizzes may **not** be made up. If an emergency forces you to miss a test, permission to be excused should be sought from me in advance, if possible. If granted, the final exam score will replace the score of the missed midterm. Final exams cannot be missed, cannot be taken before nor taken after the date scheduled by the registrar's office.

Academic Integrity:

Cheating is a serious academic crime. Oakland University policy requires that all suspected instances of cheating be reported to the Academic Conduct Committee for adjudication. Anyone found responsible of academic misconduct in this course may receive a course grade of 0.0, in addition to any penalty assigned by the Academic Conduct Committee. Students should read the Academic Conduct Regulations of Oakland University.

Working with others on homework is not cheating unless indicated by the instructor; handing in an assignment that has essentially been copied from someone else is cheating. Looking at someone else's work during an exam is cheating. Receiving help from someone else or consulting unauthorized material during an exam is cheating. Providing such assistance for someone else also constitutes cheating.