MA480 – Introduction to Cryptography

Instructor: Steven Jackson
Office: Sci-3-082
E-mail: jackson@math.umb.edu
Phone: (617) 287-6469
URL: www.math.umb.edu/~jackson/

Course Description

This course is an introduction to the mathematics of modern computer-assisted cryptography and cryptanalysis, with emphasis on public-key cryptosystems. Major topics include cryptosystems based on discrete logarithms (e.g. Diffie-Hellman and ElGamal), integer factorization (e.g. RSA), and elliptic curves (e.g. Elliptic Diffie-Hellman and Elliptic ElGamal), as well as algorithms facilitating attacks on these systems (e.g. the Pohlig-Hellman algorithm and various factorization algorithms). Additional topics may, if time permits, include: elements of information theory, symmetric cryptosystems of contemporary relevance such as AES, and digital signatures.

Prerequisites

Students should be conversant with elementary number-theoretic concepts such as divisibility and primeness. In addition, they should be capable of rapidly absorbing the definitions of fundamental algebraic structures such as groups and fields. Some familiarity with linear algebra will be helpful at various points.

Text

There is one required text for the course: *An Introduction to Mathematical Cryptography*, by Jeffrey Hoffstein, Jill Pipher, and Joseph H. Silverman (there is only one edition).

Grading

Course grades are based on two mid-term examinations (25% each) and a comprehensive final exam (50%). However, students who wish to do so may replace the final exam by a major coding project: writing a toy cryptosystem that implements all of the major algorithms discussed in class (an official list will appear on the course web page as the semester proceeds).

Reading and class preparation

There is a reading assignment associated with each class period. Although it is not generally possible to discuss every topic in class, students are responsible

for the entire content of the reading assignment. *Test and exam questions may cover reading material not discussed explicitly in class.* Consequently it is very important to complete the reading assignments on time and to come to class prepared with questions.

Make-up tests

Tests may be rescheduled only in cases of serious illness, bereavement, or other circumstances of similar gravity. Whenever possible, arrangements for make-up tests must be made *in advance* of the regularly scheduled testing time.

Student conduct

Students are required to adhere to the University Policy on Academic Standards and Cheating, to the University Statement on Plagiarism and the Documentation of Written Work, and to the Code of Student Conduct as delineated in the catalog of Undergraduate Programs, pp. 44–45 and 48–52. The Code is available online at the following web site:

`http://www.umb.edu/editor_uploads/images/life_on_campus/CSC.pdf`

Web page

This syllabus and other course materials are available on-line at

`http://cartan.math.umb.edu/wiki/index.php/Math_480,_Spring_2015`

Course Calendar

Homework problems should be done prior to the due date but ***are not to be handed in.***

Thursday, January 29: Introduction. Substitution ciphers.

Tuesday, February 3: GCDs and the Extended Euclidean Algorithm.

Read before class: Sections 1.1 and 1.2.

Do before class: Assignment 1.

Thursday, February 5: Modular arithmetic.

Read before class: Section 1.3.

Tuesday, February 10: Unique factorization. Powers and primitive roots in finite fields.

Read before class: Sections 1.4 and 1.5.

Do before class: Assignment 2.

Thursday, February 12: Symmetric and asymmetric ciphers.

Read before class: Sections 1.6 and 1.7.

Tuesday, February 17: Discrete logarithms.

Read before class: Sections 2.1, and 2.2.

Do before class: Assignment 3.

Thursday, February 19: Diffie-Hellman key exchange and the ElGamal cryptosystem.

Read before class: Sections 2.3 and 2.4.

Tuesday, February 24: Overview of groups. Estimating the difficulty of the discrete logarithm problem.

Read before class: Sections 2.5 and 2.6.

Do before class: Assignment 4.

Thursday, February 26: A collision algorithm for the DLP. The Chinese Remainder Theorem.

Read before class: Sections 2.7 and 2.8.

Tuesday, March 3: The Pohlig-Hellman algorithm.

Read before class: Section 2.9.

Do before class: Assignment 5.

Thursday, March 5: Rings, quotients, and finite fields.

Read before class: Section 2.10.

Tuesday, March 10: Euler's formula and roots modulo pq.

Read before class: Section 3.1.

Do before class: Assignment 6.

Thursday, March 12: Exam 1 (assignments 1–5).

Tuesday, March 24: The RSA cryptosystem.

Read before class: Sections 3.2 and 3.3.

Do before class: Assignment 7.

Thursday, March 26: Primality testing.

Read before class: Section 3.4.

Tuesday, March 31: Pollard's $p-1$ algorithm.

Read before class: Section 3.5.

Do before class: Assignment 8.

Thursday, April 2: Factorization via difference of squares.

Read before class: Section 3.6.

Tuesday, April 7: Smooth numbers and sieves.

Read before class: Section 3.7.

Do before class: Assignment 9.

Thursday, April 9: More on smooth numbers and sieves.

Tuesday, April 14: The index calculus and discrete logarithms.

Read before class: Section 3.8.

Do before class: Assignment 10.

Thursday, April 16: Exam 2 (assignments 6–9).

Tuesday, April 21: Quadratic residues and quadratic reciprocity.

Read before class: Section 3.9.

Do before class: Assignment 11.

Thursday, April 23: Probabilistic encryption.

Read before class: Section 3.10.

Tuesday, April 28: Elliptic curves.

Read before class: Section 5.1.

Do before class: Assignment 12.

Thursday, April 30: Elliptic curves over finite fields. The ECDLP.

Read before class: Sections 5.2 and 5.3.

Tuesday, May 5: Elliptic curve cryptography.

Read before class: Sections 5.4 and 5.5.

Do before class: Assignment 13.

Thursday, May 7: Lenstra's elliptic curve factorization algorithm.

Read before class: Section 5.6.

Tuesday, May 12: Review.

Do before class: Assignment 14.