Course information and syllabus for Math 445 Introduction to Cryptography Spring 2004

Course overview

Cryptography is about the design and analysis of algorithms and protocols to protect communications from eavesdroppers. It is widely employed in commercial, military, diplomatic, and internet applications. This course is an introduction the mathematical aspects of cryptography.

Contact Information:

- **Professor:** Douglas Ulmer, Professor of Mathematics
  - **Office:** Math 204
  - **Phone:** 621-6861
  - **E-mail:** ulmer@math.arizona.edu
  - **Office hours:** 2-3 Mondays, 4-4:30 Mondays and Fridays in Math 204. 1-2 Fridays in Math East 145.
- **Assistant:** Cetin Urtis, Visiting Assistant Professor of Mathematics
  - **Office:** Math 305
  - **Phone:** 621-9991
  - **E-mail:** urtis@math.arizona.edu
  - **Office hours:** 12-1 Mondays, 3-4 Tuesdays, 10-11 Wednesdays in Math 305.

- **Course Homepage:** http://math.arizona.edu/~ulmer/teaching/CrypS04/index.html

Course Policies:

- **Attendance:** Students are expected to attend every scheduled class, and to be familiar with the University Class Attendance policy as it appears in the General Catalog. It is the student's responsibility to keep informed of any announcements, syllabus adjustments or policy changes made during scheduled classes. Students who are excessively absent may be "administratively dropped" from the course. "Excessively" means 2 days in a row or any 3 days during the semester.
- **Homework:** Homework is an essential component of the course and will be assigned and collected regularly, approximately weekly. For full credit, homework must be turned in at the beginning of class on the day it is due. Late homework will be accepted for grading until the beginning of the next class meeting, but will earn only 70% credit. Homework turned in later *may* be graded but will earn no points. The single lowest homework score will be thrown out before calculating the final homework score.
- **Project:** Each student will complete a required project, which may entail analyzing a cryptosystem or decrypting an encrypted message using tools discussed in class, implementing some interesting cryptogrpahic protocol or tool, or writing an expository paper about an issue of current cryptographic interest. More details will be provided later.
- **Exams:** There will be one in-class exam during the first half of the semester and a final exam.
- **Dates:** The test is tentatively scheduled for **March 3**. The project will be due approximately **April 23**,

and the University has scheduled the final exam for **May 7 from 2:00 - 4:00 in Modern Languages 314**. The dates of the exam and project may change but the date of the final exam will definitely not change. Exams cannot be given at any other time. If a test or project is missed for a valid reason, the score for that test will be replaced with the score on the corresponding part of the final exam. (The meanings of "valid" and "corresponding part" will be determined by the instructor.) A second missed test or project, or a missed final exam, will result in a score of 0. There will be no exceptions to this policy.

- **Grades:** Course grades will be determined by scores on exams, projects, and homework, with weights as follows: Homework, 25%, midterm exam 20%, project 20%, final exam 35%. Grades will be based on the percentage of possible points earned, and will be no lower than these: 90-100%: A, 80%-90%: B, 70%-80%: C, 60%-70%: D, below 60%: E.
- **W's and I's:** Students withdrawing from the course before March 9 will receive the grade W if they are passing at the time. Students will be considered to be passing at the time of withdraw if they have scored at least 50% on the work completed at that time.
  The grade of I will be awarded only if all of these conditions are met:
  1. The student has completed all but a small portion of the required work.
  2. The student has scored at least 50% on the work completed.
  3. The student has a valid reason for not completing the course on time.
  4. The student agrees to make up the material in a short period of time.
  5. The student asks for the incomplete before the final exam.

Syllabus

- **Text:** "Introduction to Cryptography" by W. Trappe and L. Washington (required). We will cover Chapters 1-7, 14, 17, and a selection from 8-13 (not in that order).
- **Software:** Many homework assignments will involve tasks, such as manipulating large numbers, that are only reasonable to do with a computer. Thus students will need to have access to a computer and a suitable software package. The following packages are highly recommended: Mathematica, Maple, Matlab. Mathematica and Matlab are available to users of the University u-system. Matlab is available on open access computers in several labs, including the information commons area of the main library. Student versions of all three packages are available at CATS for about $125. *Students are responsible for getting access to and learning to use a suitable package.* Instructions in the appendices to the Trappe-Washington text should be enough to get you started in Mathematica, Maple, or Matlab.
- **Topics:**

Dates	Topic
1/14 - 1/30	Basic framework and examples (TW Chapters 1-2)
2/2 - 2/6	Number Theory I (TW 3.1-3.4, 3.10)
2/9 - 2/20	Symmetric Key Cryptography (TW Chapters 4-5)
2/23 - 2/27	Information Theory (TW Chapter 14)
3/1 - 3/5	Review and Midterm
3/8 - 3/12	Number Theory II (TW 3.5 - 3.9)
3/22 - 4/2	Public Key Cryptography (TW Chapters 6-7)
4/5 - 4/9	Quantum Computing (TW Chapter 17)
4/12 - 5/5	Selected Applications (TW Chapters 8, 13, and parts of 9-12)