Math 445, Introduction to Cryptography
Course Syllabus
Summer 2 2016

Instructor Contact Information

Instructor: Dr. Katie Walsh
Office: Math 305
Office Hours: M 1-2:30 and W 11-12:30
Email: k3walsh@math.arizona.edu
Phone: 520-626-3279

General Information

Course Description: Introduction to cryptosystems and cryptanalysis. Basic number theory and finite fields. Basic complexity theory and probability. RSA and Diffie-Hellman protocols, factorization and discrete log attacks. Advanced encryption standard. Additional topics as times allows.

Prerequisites: Appropriate Math Placement Level or MATH 215 or MATH 313. Ability to program in C, Java or Python OR willingness to learn to work with MATLAB.

Course Objectives:

1. MATH 445 is a concrete introduction to cryptography. The main purpose of the course is to introduce students to the mathematics underlying various cryptosystems in both symmetric key and public key cryptography.

2. Students will also practice coding and decoding messages using computers.

3. A mild introduction to mathematical reasoning and proofs is a secondary goal.

Required Textbooks and Materials:
The text is *Introduction to Cryptography with Coding theory, second edition*; Trappe- Washington, Pearson Prentice Hall.

Students will also need access to a computer with either MATLAB or another computer programming language they have experience with. MATLAB is available to students for free.

Course website/D2L site: http://d2l.arizona.edu and Piazza

Communication with Students

Announcements and important course information may be sent out via official University email or through D2L and/or Piazza. It is the student's responsibility to check for messages and announcements regularly.

Accessibility and Accommodations

It is the University's goal that learning experiences be as accessible as possible. If you anticipate or experience physical or academic barriers based on disability or pregnancy, please let me know immediately so that we can discuss options. You are also welcome to contact Disability Resources (520-621-3268) to establish reasonable accommodations.

Please be aware that the accessible table and chairs in this room should remain available for students who find that standard classroom seating is not usable.

Attendance/Administrative Drops

Daily attendance is expected from every student. Students who miss the first class meeting will be administratively dropped unless they have made other arrangements. In addition, students with more than 3 unexcused absences may be administratively dropped from the course. (See Administrative Drop Policy at `http://catalog.arizona.edu/2015-16/policies/classatten.htm`) If you need to miss class for unavoidable circumstances, contact your instructor as soon as possible. Please note the following:

- All holidays or special events observed by organized religions will be honored for those students who show affiliation with that particular religion,
- Absences pre-approved by the UA Dean of Students (or Dean's designee) will be honored.

It is the student's responsibility to notify the instructor in advance of an absence related to religious observation or an activity for which a Dean's excuse has been granted, and to arrange for how any missed work will be handled.

Academic Integrity

Students are responsible to inform themselves of University policies regarding the Code of Academic Integrity. Students found to be in violation of the Code are subject to penalties ranging from a loss of credit for work involved to a grade of E in the course, and risk possible suspension or probation. The Code of Academic Integrity will be enforced in all areas of the course, including, but not limited to, homework, quizzes, and tests. For more information about the Code of Academic Integrity policies and procedures, including information about your rights and responsibilities as a student, see the following website: `http://deanofstudents.arizona.edu/academic-integrity/students/academic-integrity`

Student Code of Conduct

Students at The University of Arizona are expected to conform to the standards of conduct established in the Student Code of Conduct. Prohibited conduct includes:

1. All forms of student academic dishonesty, including cheating, fabrication, facilitating academic dishonesty, and plagiarism.

2. Interfering with University or University-sponsored activities, including but not limited to classroom related activities, studying, teaching, research, intellectual or creative endeavor, administration, service or the provision of communication, computing or emergency services.

3. Endangering, threatening, or causing physical harm to any member of the University community or to oneself or causing reasonable apprehension of such harm.

4. Engaging in harassment or unlawful discriminatory activities on the basis of age, ethnicity, gender, handicapping condition, national origin, race, religion, sexual orientation, or veteran status, or violating University rules governing harassment or discrimination.

Students found to be in violation of the Student Code of Conduct are subject to disciplinary action. For more information about the Student Code of Conduct, including a complete list of prohibited conduct, see the following website: `http://deanofstudents.arizona.edu/accountability/students/student-accountability`

Other Relevant University Policies Relating to Conduct

Please take note of the following University policies:

• Policy on Threatening Behavior by Students: `http://policy.web.arizona.edu/education-and-student-affairs/threatening-behavior-students`

• Nondiscrimination and Anti-Harassment Policy: `http://policy.arizona.edu/human-resources/nondiscrimination-and-anti-harassment-policy`

Expected Classroom Behavior

Students should turn off all electronic devices during class unless the device is deemed necessary for the class by the instructor. This includes, but is not limited to cell phones, mp3 players, and laptops. If you have a disability-related accommodation that involves the use of a computer during class, please discuss this with your instructor in advance.

Homework & Quiz Policies

There will be both written and computer based homework assignments. Written homework will be due in class on Friday. Each written homework with be worth 25 points for a total of 100 points. There will also be a computer portion of each assignment. You will have a choice between with either MATLAB questions or writing your own computer code in a language you know. Each computer assignment is worth 15 points for a total of 60 points. There is an opportunity to replace computer homework points by completing code breaking challenges throughout the course. These points will replace computer assignment points and will NOT count as extra credit once the 60 points in reached.

There will be short in class quizzes on Tuesday and Thursday. Questions will be similar, but not exactly the same, as the homework due the coming Friday. Completing your homework early is a great way to prep for the quiz. There will be 9 quizzes total. Each quiz is worth 5 points. The lowest quiz grade will be dropped. Quizzes are worth a total of 40 points.

Midterm Exams

There will be in class midterm exams on Friday, July 22 and Wednesday, August 3. Makeup Exams will only be given in extenuating circumstances at the discretion of the instructor. If you miss an exam, you must contact the instructor via e-mail within 24 hours to discuss the possibility of a make-up. Make-ups with automatically be penalized 10% of the earned grade. If you are late to an exam, you will be allowed the entire time allotted for the exam, but extra time will also be penalized at the prorated rate and must be immediately following class.

Any academic integrity violation related to an exam will result in a grade of 0 on that exam and a referral to the disciplinary board.

Final Exam

Final Exam Date: Wednesday, August 10, 2016

Final Exam Location: Regular Classroom

Please note the following:

- University rules relating to final examinations may be found at: `http://www.registrar.arizona.edu/schedule101/exams/examrules.htm`

Missed Exam Policy

Students who are unable to attend an exam should notify their instructor as soon as possible. Arrangements for a make-up test will be considered on a case by case basis. Make-up exams will be administered only at the discretion of the instructor. If a student is allowed to make up a missed exam, (s)he must take it at a mutually arranged time. No further opportunities will be extended. Failure to contact the instructor as stated above will result in a grade of zero on the exam.

Calculation of Course Grades

The various components of the course grade will be weighted as follows:
Midterm Exam 2 x 75 = 150 points
Homework: Written and Computer Homework 160 points
Quizzes: 40 points
Final Exam: 150 points
Course grades will be calculated based on the following scale: 90-100% A, 80-89.99% B, 70-79.99% C, 60-69.99% D, Below 60% E

A grade of "I" (Incomplete) will be given only at the instructor's discretion, according to University Policy as described at `http://www.registrar.arizona.edu/gradepolicy/incomplete.htm`.

Grading Disputes

Any grading disputes must be addressed within one week after an exam or homework has been returned.

Withdrawal

A student may withdraw from the course with a deletion from record through July 14, 2016, using UAccess. A student may withdraw with a grade of "W" through July 30, 2016, using UAccess.

Changes to the Course Syllabus

The information contained in the course syllabus, other than the grade and absence policies, may be subject to change with reasonable advance notice, as deemed appropriate by the instructor.

Tentative Weekly Schedule

See next pages.

Math 445 **Jul 2016 (Mountain Time - Arizona)**

Sun	Mon	Tue	Wed	Thu	Fri	Sat
10	11 Chapter 1 and	12 3.1-3.3 Quiz 1	13 (read 2.5 and 2.3-2.4	14 3.7 3.8 and 2.7 Last day to Quiz 2	15 2.8,2.9, 2.11	16
17 Cryptography	18 Section 3.4, 3.5	19 3.6 3.7 Quiz 3	20 3.9, (3.10)	21 3.11, Review Quiz 4	22 Exam 1	23
24	25 Chap 4 Intro to Ch 5	26 5.2, 5.3 Quiz 5	27 5.4 6.1	28 6.2,6.3 Quiz 6	29 6.4	30 Last day to
31	1 6.5,6.6	2 6.7 Quiz 7 review	3 Exam 2	4 7.1,7.2 8.4 Quiz 8	5 7.3,7.4	6

Math 445 **Aug 2016 (Mountain Time - Arizona)**

Sun	Mon	Tue	Wed	Thu	Fri	Sat
31	1 6.5,6.6	2 6.7 Quiz 7 review	3 Exam 2	4 7.1,7.2 8.4 Quiz 8	5 7.3,7.4	6
7	8 7.5 Quiz 9	9 review	10 Final	11	12	13