MATH 314
Introduction to Cryptography
Class Policies

Mike O'Leary
Office: YR 317
Office Phone: 410-704-4757
Email:moleary@towson.edu

Fall 2019
Class: TuTh 5:00-6:15
Room: YR 129
Section: 102
Office Hours: Tu 10-11, Th 1-2, and by appointment

Prerequisites: COSC 236; either MATH 263 or MATH 267; and either MATH 330 or MATH 331 (may be taken concurrently).

Catalog Description: A broad introduction to cryptography and its mathematical foundations: Elementary number theory; classical and modern symmetric key cryptosystems; public key cryptography; primality tests, factoring algorithms; hash functions and digital signatures. Selected further topics may include security protocols, digital cash, elliptic curve cryptography, or quantum cryptography.

Instructional Material: The primary assigned text is W. Trappe and L.C. Washington, *Introduction to Cryptography with Coding Theory*, Pearson, Second edition, 2006.

Students are expected to write their own code for homework. The class presentations will use Python 3.7. For their assignments, students can use Python (2.x or 3.x), C, C++, Java, Mathematica, Matlab, or Octave. If a student wishes to use different language, please see me.

Methods of Instruction: Class time will be devoted to lectures and, where appropriate, time for joint work on assigned projects.

Learning Outcomes:

- Students will be able to calculate using classical cryptosystems: shift, affine, Vigenère, and block ciphers. Encryption, decryption, and attacks against these systems.
- Students will be able to use and to prove results from number theory needed for cryptography. The Chinese Remainder Theorem, modular exponentiation, and Legendre symbols. Students will be able to construct and compute with finite fields.
- Students will understand DES, and be able to manually encrypt and decrypt data encoded with a simplified DES. Students will be able to perform differential cryptanalysis on a three round simplified DES system.
- Students will be able to encrypt and decrypt data encoded with AES.
- Students will be able to encrypt and decrypt data encoded with RSA. Students will be able describe common attacks against RSA.
- Students will be able to compute hash functions and describe common attacks against hash functions.
- Students will be able to compute RSA and ElGamal signatures.
- Students will be able to perform arithmetic operations on elliptic curves, and will be able to use library functions to encrypt and decrypt data encoded with an elliptic curve cryptosystem.

Attendance: Attendance is expected; you should only miss a class for a compelling reason. If you do miss a class, you are responsible for any material that you miss, including any homework assignments given in that class. Unexcused absences can result in a lower grade.

Note that class will meet at its regular time (5:00-6:15) on Tuesday, November 26 prior to Thanksgiving. Attendance is expected. The material covered in this class time will appear on the final exam.

Grading: A number of problem sets will be posed to the class. Students will need to prepare written solutions for each of these problems, and these problems will be graded. These written solutions must be turned in before the corresponding class discussion of the solution for the solution to receive full credit. Together, all of these problems will account for 35% of the student's final grade.

There will be two midterm examinations; each will be worth 15% of the student's final grade.

There will be one final examination. It will be held on Thursday, December 12 from 5:15-7:15 in YR 129. The final examination will count for 35% of the student's final grade.

Given a final point score p, final grades will be assigned based on the following scheme

- $85 \leq p$: A
- $83 \leq p < 85$: A-
- $82 \leq p < 83$: B+
- $75 \leq p < 82$: B
- $73 \leq p < 75$: B-
- $72 \leq p < 73$: C+
- $65 \leq p < 72$: C
- $55 \leq p < 65$: D
- $p < 55$: F

Guidelines for Homework:

1. Late work will not be accepted without a compelling reason.
2. Assignments are required to be neat, clean, and paper-clipped or stapled.
3. Assignments must include the author's name, and a brief description of the assignment.

Any assignment that does not meet these criteria may receive a deduction in score, or more generally will simply be rejected.

Academic Integrity The nature of higher mathematics requires that students adhere to accepted standards of academic integrity. Violations of academic integrity include cheating, plagiarism, falsification and fabrication, complicity in academic dishonesty, personal misrepresentation and proxy, bribes, favors and threats. Cheating is a serious offense that will have grave consequences for your academic life.

Many homework problems require the development of a computer program. Students may use code from external sources provided the original source is explicitly credited. (A note with a URL to the source will be sufficient.)

Students are allowed to discuss homework problems with their classmates, however all work that is turned in must be the student's own work. If multiple students work together on a problem, their answers must explain the contribution of each student.

Students who violate these standards will either fail the course outright or, at the instructor's discretion, may merely receive a zero on any assignment for which the student receives inappropriate assistance. All violations of these standards will be referred to the administration for possible additional action.

Tentative Schedule:

- Week 1 (8/26): 2.1-2.4, 2.7, 2.8. Classical cryptosystems. Shift, affine, Vigenère, Substitution, and Block ciphers. Diffusion and confusion. ASCII, UTF-8, UTF-16.
- Week 2 (9/2): 3.1, 3.2, 3.3, Modular arithmetic, and the Euclidean algorithm.
- Week 3 (9/9): 3.4, 3.5, 3.6, 3.7, Chinese Remainder Theorem, modular exponentiation, primitive roots.
- Week 4 (9/16): 4.1, 4.2, 4.3, Feistel Ciphers, simplified DES, differential cryptanalyis.
- Week 5 (9/23): 4.3, 4.4, 4.5 Differential Cryptanalyis (ctd), DES, modes of operation.
- Week 6 (9/30): 4.4, 4.5, 4.7, Breaking DES, meet in the middle attacks.
- Week 7 (10/7): 3.11, Finite fields. **Exam # 1**.
- Week 8 (10/14): 3.11, 5.2, 5.3, Finite fields, AES.
- Week 9 (10/21): 3.10, 3.12, 6.1, Legendre and Jacobi symbols, continued fractions, RSA.
- Week 10 (10/28): 6.2, 6.3, 6.4, Attacks on RSA. Solovay-Strassen and Miller-Rabin Primality Tests, Dixon's Factorization Algorithm.
- Week 11 (11/4): 7.1, 7.2, 7.4, 7.5, Discrete Logarithms, Diffie-Hellman, El Gamal.
- Week 12 (11/11): 8.1, 8.2, 8.3, 8.4. MD4, MD5, SHA-1, SHA2-256, SHA3-256. Attacks on hash functions.
- Week 13 (11/18) : 16.1, Elliptic curves. **Exam # 2**.
- Week 14 (11/25): (Thanksgiving week) 16.2 Elliptic curves mod p.
- Week 15 (12/2): 16.3, 16.4, 16.5, Elliptic curve cryptosystems

Withdraw: The last day to withdraw from the course with a grade of W is November 4.

Course repeat policy: Students may not repeat a course more than once without prior permission of the Academic Standards Committee.

Students with Disabilities: This course is in compliance with Towson University policies for students with disabilities. Students with disabilities are encouraged to register with Disability Support Services (DSS), 7720 York Road, Suite 232, 410-704-2638 (Voice) or 410-704-4423 (TDD). Students who expect that they have a disability but do not have documentation are encouraged to contact DSS for advice on how to obtain appropriate evaluation. A memo from DSS authorizing your accommodation is needed before any accommodation can be made.

Department of Mathematics Commitment to Diversity: Towson University values diversity and fosters a climate that is grounded in respect and inclusion. Everyone participating in this course is expected to treat all others in accordance with this vision and policy. TU's diversity tenets include sex, sexual orientation, race and ethnicity, color, nationality, gender identity or expression, mental/physical ability, religious affiliation, age, and veteran status. If you feel these expectations have not been met, please contact the Math Department's Diversity representative, Dr. Goode at egoode@towson.edu.

Help: You are welcome to stop by my office, for whatever reason, and at whatever time, even if there are no office hours scheduled then.

Reading: If you have gotten this far, here is your first homework assignment. Tell me a bit about yourself- why you are taking this class, when will you graduate, and what you want to do after

graduation. Hand it in at the start of the first class, but do not say anything out loud. Free points for those, like you, who pay attention!