MATH 314
Introduction to Cryptography

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

Fall 2020
Class: TuTh 5:00-6:15
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 Heiko Knospe, *A Course in Cryptography*, American Mathematical Society, 2020.

Students are expected to have access to SageMath `https://www.sagemath.org/`. This can be installed locally on a student's computer. Alternatively, students can use CoCalc `https://cocalc.com` which is a shared cloud platform that provides access to SageMath.

Students will also need to write their own computer programs; programs not written in SageMath should be written in Python 3.7 `https://www.python.org/`.

Methods of Instruction: This will be a fully online class, taught in a flipped format.

- Students will come to class having read the week's assigned material.
- Students will come to class having solved (or having attempted to solve) individually the Reading Questions
- During the first class of the week, the instructor will present a short 5-10 minute overview of important topics
- On (or before) the first class of the week, the instructor will distribute a hand-out (electronically) with examples and key notes
- During the first class of the week, once the instructor introduction is complete, the students will work in groups to refine their answers to the Reading Questions.
- In the second class of the week students will work in groups on the Discussion Questions
- Each week will include either individual homework assignments or group projects.

Learning Outcomes:

- Students will understand encryption schemes and definitions of security. Students will be able to evaluate an encryption scheme to determine if it has perfect security or if it vulnerable to various attacks, including eavesdropping, chosen plaintext, and chosen ciphertext attacks.
- Students will be able to use and to prove results from number theory needed for cryptography.
- Students will be able to perform computations using algebraic structures including cyclic groups and finite fields.

- Students will be able to construct AES, and encrypt and decrypt data encoded with AES.
- Students will be able to construct stream ciphers including linear feedback shift register ciphers, RC4, Salsa20 and Chacha20.
- Students will be able to construct cryptographic hash functions using either the Merkle-Damgård construction or a Keccak sponge, including SHA-1, SHA-2, and SHA-3.
- 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 use Diffie-Hellman algorithms and discrete logarithms for key exchange.
- Students will be able to implement message authentication codes (MAC).
- 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 in a course that is fully online is evaluated differently. Online attendance is more than just logging into the course or being physically present. Attendance is measured by your intellectual and active engagement with the course content, course tools, course instructor, and with other students in the course.

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 assignments. Unexcused absences will result in a lower grade.

Grading: Final grades will be calculated by weighting the results from the following categories:

- Individual Reading Questions: 20%
- Group Reading Questions: 20%
- Group Discussion Questions: 20%
- Individual Homework: 20%
- Group Projects: 20%

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

Late work will not be accepted without a compelling reason.

Student Resources: Collaboration: A shared OneDrive site will be used for class notes, assignments, and the like. Details will be provided by email.

Student Resources: Writing Mathematics: There are several ways to write mathematics, with the most professional being LaTeX.

Group work will be done using Microsoft Word. The shared OneDrive site will be used during class time to hold the shared documents, so the instructor can move from one group to another and see what each group is doing.

Instructions on how to use the equation editor in Microsoft Word are available at `https://en.wikibooks.org/wiki/Typing_Mathematics_in_Microsoft_Word`.

Student Resources: Gradescope: The final versions of student assignments will be in .pdf format, and submitted via Gradescope `https://www.gradescope.com`. Further instructions will be provided in class.

Student Resources: Discussion Board: There will be a Discord site `https://discord.gg/FmkMkha` for student discussions. This will be shared across all three sections of this course this semester.

Instructors will be available to answer public questions on the discussion board as schedule permits. Students with private questions should take them to Office Hours or email directly to the instructor.

Office Hours: Office hours will be through Zoom.

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.

The pandemic and online education may have made cheating easier, but they *do not make it right*. Many of you may wish to enter the field of cybersecurity. Many jobs in cybersecurity require a clearance, and nearly all require *trust*. Professionals that are discovered to cheat often lose their jobs.

Group assignments can be discussed with members of your group, but not with other groups or students outside class. Individual assignments should not be discussed with other students.

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. Although copying and properly crediting copying code is not an academic integrity violation, it can result in a lower grade on an assignment.

The instructor is familiar with common cheating sites, which will not named. Be assured that the content of these sites is monitored, and their use is a violation of the academic integrity policy.

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 A tentative course schedule is included in a separate document.

Withdraw: The last day to withdraw from the course with a grade of W is November 2.

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.

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 electronically before the first class, but do not announce this to the class. Free points for those, like you, who pay attention!