Cryptography COMP 150CRY (COMP 150-01 / MATH 190-02) MW 6:00 - 7:15 PM (M+ Block)

Instructor: David Wittenberg mailto:dkw@cs.tufts.edu
Office Hours: Monday 7:30-8:30pm; Wednesday 4:45-5:45pm

TA: Christopher Ratigan mailto:Christopher.Ratigan@tufts.edu
Office Hours: Tuesday and Wednesday 2-3 pm.

Canvas home https://canvas.tufts.edu/courses/27291 Contact the instructor for access to Canvas.

Textbook: *Introduction to Cryptography with Coding Theory* (third edition) 2020 by Wade Trappe and Lawrence Washington; Pearson Publishing

Purchasing the Textbook:
eText platform ISBN 978-0-13-526016-6 Direct cost is $79.99 (1-year access).

The access code for the book may be in the bookstore as ISBN: 978-0-13-485906-4

Also available: Rental (normal bound edition): ISBN: 978-0-13-673154-2 $64.99 At the end of the term, you can purchase the book, but I don't know at what price.

There are also two editions listed that I have not found for sale:

- Loose Leaf edition (you supply the binder): ISBN: 978-0-13-486099-2
- Purchase (normal bound edition): ISBN: 978-0-13-486099-2

The eText and rental editions are available from the following URL: This allows purchase directly from Pearson using the following URL:
https://www.pearson.com/store/p/introduction-to-cryptography-with-coding-theory/P1000010329

It should be possible for you to see my annotations in the text if you use the eText version. Contact the instructor for access information.

Prerequisites: COMP 160, COMP 170, graduate standing, a 100 level MATH course, or permission of the instructor.

Course Description: This is a introduction to cryptography, starting with the first ciphers, and leading up to present day issues. We will discuss how codes and ciphers work, and how they can be broken. We will cover both Private key (Symmetric) and Public Key (Asymmetric) cryptography. Topics include: cryptographic protocols, using block ciphers, methods for key exchange, hashing, message authentication, digital signatures, secret sharing, and digital cash. We will use a mathematical approach to prove properties about the crypto systems we study.

Course Outline: (Note: Schedule is approximate.)
Week:

1. - Introduction
   - Models
   - Pre-computer Cryptosystems
     - Skytale Cipher
     - Shift Cipher
     - Affine Cipher
     - Substitution Cipher
     - Vigenère Cipher
     - Beale Cipher
     - Enigma – the ultimate Vigenère Cipher
   - Cryptanalysis of Simple Cryptosystems
     - Cryptanalysis of Shift Cipher
     - Cryptanalysis of Affine Cipher
     - Cryptanalysis of Substitution Cipher
     - Cryptanalysis of Vigenère Cipher
     - Cryptanalysis of Transposition Cipher
   - Bayes' Theorem
2. - Information Theory
   - Entropy
   - One Time Pad
   - Perfect Secrecy (Information Theoretic Security)
3. Block Ciphers
   - DES
   - AES
   - Groups, Rings, Fields
   - Modes of Block Ciphers
4. RSA
5. - Discrete Logarithm
     - Calculating Discrete Logarithm
     - Index Calculus
   - ElGamal Cryptosystems
6. - Hash Functions
     - Randomness and Pseudo Randomness
     - Secure Hash Functions
     - MAC (Message Authentication Codes)
       * Merkle-Damgaard
       * Keccak
7. - Secret Sharing
   - Midterm
8. - Cryptographic protocols
     - Diffie Helman Key Exchange
     - Quadratic Residue
     - Goldwasswer & Micali
9. Elliptic Curve & other second generation public key systems
10. - Zero-knowledge proofs
    - Signature Schemes

11.
    - Post Quantum
    - Random Numbers
    - Practical Shamir Sharing
12.
    - Certificate Authorities
    - Politics
13. Practical attacks

Required Reading:

- New Directions in Cryptography by Whitfield Diffie and Martin Hellman in *IEEE Transactions on Information Theory* November 1976. available at
  `https://ee.stanford.edu/~hellman/publications/24.pdf`
- Mathematical Games: A new kind of cipher that would take millions of years to break by Martin Gardner in *Scientific American* August 1977 available at
  `https://simson.net/ref/1977/Gardner_RSA.pdf`
- A method for Obtaining Digital Signatures and Public-key Cryptosystems by Ron Rivest, Adi Shamir, and Len Adleman in *Communications of the Association for Computing Machinery* 1978. available at
  `https://people.cs.umass.edu/~emery/classes/cmpsci691st/readings/Sec/Rsapaper.pdf`
- How to Share a Secret by Adi Shamir in *Communications of the Association for Computing Machinery* November 1979. available at
  `http://users.cms.caltech.edu/~vidick/teaching/101_crypto/Shamir1979.pdf`
- Cryptography and Cryptographic Protocols by Oded Goldreich in *Distributed Computing* September 2003. available at
  `http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.117.3618&rep=rep1&type=pdf`
- Zero Knowledge Proofs: An illustrated primer by Matthew Green. November 2014. available at:
  `https://blog.cryptographyengineering.com/2014/11/27/zero-knowledge-proofs-illustrated-p`

Recommended Reading:

- The American Black Chamber by Herbert Yardley. 1931.
  Still available in paperback. A history of code breaking in the 1920s by the head of the American code breaking agency.
- The Code Breakers by David Kahn.
  The 1967 edition is the classic description of cryptographic history. Completely non-technical. Barely covers computer-related cryptography. There's an updated 1996 edition.
- The Code Book: The Science of Secrecy from Ancient Egypt to Quantum Cryptography by Simon Singh. 1999.
  A history of encryption with the math explained for a popular audience. Fascinating history. Less complete and more up to date than Kahn's book.

- Crypto: How the Code Rebels Beat the Government – Saving Privacy in the Digital Age by Steven Levy. 2001.
  History of computer-based Cryptography. Picks up where Kahn leaves off, but rather more political than Kahn or Singh.

- The Story of Alice and Bob available at:
  `http://web.mit.edu/jemorris/humor/alice-and-bob`
  A very funny description of the two main antagonists in most cryptography papers. It will only be funny after you've seen the protocol section of the course.

- Code Girls: The Untold Story of the American Women Code Breakers of World War II by Liza Mundy. 2017.
  Interesting for its description of the era. Very non-technical. Vaguely similar to *Hidden Figures*, but without the racism.

- The Mathematics of Secrets: Cryptography from Caesar Ciphers to Digital Encryption by Joshua Holden. 2017.
  The mathematics behind cryptography. Requires mathematical thinking, but no math beyond high school.

- How to Explain Zero-Knowledge Protocols to Your Children by Jean-Jacques Quisquater *et al.*
  A fable to describe zero-knowledge proofs. Rather fun, and technically correct. available at:
  `http://pages.cs.wisc.edu/~mkowalcz/628.pdf`

Other Texts: Other textbooks on the subject. You may find it helpful to consult one of them if you find our text isn't clear.

- The Joy of Cryptography by Mike Rosulek 2021. available at:
  `https://web.engr.oregonstate.edu/~rosulekm/crypto/` A short textbook that covers much of what we cover. It uses more intuition and less mathematics than our text, so you may find it a good place to look for a general understanding.

- Cryptography and Network Security by William Stallings. 2016.
  Similar in level to our text, but perhaps a bit more detailed. Puts all the math in the first two chapters. Excellent index.

- Secret History: The Story of Cryptology by Craig P. Bauer 2013. Another text about on the same level as ours, but combines history and technical detail in one narative.

- Cryptography: Theory and Practice 4th edition by Douglas Stinson and Maura Paterson, 2019. The text we used in 2019. A little more mathematical than our text.

Grading: Final grades will be calculated based on 50% homework, 35% final exam, and 15% midterm exam.

Homework: Homework will be assigned weekly, and usually be due Wednesday at 6pm (before class).

HW collaboration policy : You are welcome to talk to the Instructor, TAs or other students about HW problems, but if so please follow the "sandwich" rule: first read and think about the problem by yourself, then work with others if desired, and then *the final form that you turn in for grading should be written by you alone using your own words.* You should not be looking up hw solutions on the Internet. If you have substantially collaborated with other students on a problem, please acknowledge this at the top of that problem, i.e. "I worked with Alex and Robin". The write up still needs to be your own. In general, you should assume that problems require justification—no credit for correct answers with no justification.

This policy is copied from COMP 61, so you are probably familiar with it.

Extra Help: Dot not hesitate to come to my office hours to discuss a homework problem or any aspect of the course.

Accomodation for Students with Disabilities: Tufts University values the diversity of our students, staff, and faculty, recognizing the important contribution each student makes to our unique community. Tufts is committed to providing equal access and support to all qualified students through the provision of reasonable accommodations so that each student may fully participate in the Tufts experience. If you have a disability that requires reasonable accommodations, please contact the Student Accessibility Services office at Accessibility@tufts.edu or 617-627-4539 to make an appointment with an SAS representative to determine appropriate accommodations. Please be aware that accommodations cannot be enacted retroactively, making timeliness a critical aspect for their provision.

Last edited: January 29, 2021