Math 485: Mathematical Cryptography

Course Website: http://www.math.byu.edu/~mjgriffin/Classes/M485.17F

Instructor: Michael Griffin, 320 TMCB,
Email: Mjgriffin@math.byu.edu. Please preface the subject line with " [M485] "
Lecture: 1:00-1:50 PM MWF, 112 TMCB;
Office hours: 320 TMCB (Office) 3:00-3:50 MW or by appointment,
149 TMCB (Computer lab) 1:00-1:50 Th.
Textbook: Introduction to Cryptography with Coding Theory, Second Edition, Wade Trappe and Lawrence C. Washington, Pearson Prentice Hall, ISBN 0-13-186239-1. There is a list of known errors in the textbook online at http://www.math.umd.edu/~lcw/cryptoerrata2.pdf
Grading: Homework 30%, two midterms 20% each, final exam 30%. Grades will be available on BYU Learning Suite.

- Homework will be due on Mondays, Wednesdays, and Fridays at **4:30 PM** in the box outside my office door, or submitted by email to mjgriffin@math.byu.edu. Your three lowest homework scores will be dropped. Late homework will not be accepted.
- Two midterm exams will be held in the testing center on **October 6-9** and **November 13-15**.
- The final exam will be take-home, and due at the scheduled final exam time (**2:30-5:30 PM, Tues December 19**). The final exam will cover all material studied this semester.

Group work and Digital Dialog: You are encouraged to work together in groups, ask questions and help each other, especially within your team. However (with the exception of explicitly designated group projects), you should write up your own homework solutions and computer code (see the **Honor Code** section below). The Digital Dialog section of learning suite is a great place to ask questions that I or other students can answer. The same principle applies. Do not share or copy completed solutions or code. Copying another student's work is neither academically honest, nor will it help you master the material and perform well on exams.

Electronic devices: Computers will be necessary to complete some homework problems. On exams, only testing center calculators may be used. Office hours on Thursdays will be held in the computer lab 149 TMCB from 3:00 to 3:50 to answer computer related questions.

Prerequisites: Math 313 (linear algebra) or equivalent, or instructor's consent. Math 371 is recommended. Some prior experience with programming and with a computer algebra system such as Sage, Maple, or Mathematica is desirable, but not essential.

Course Description: This is a course in the mathematics and algorithms of modern cryptography. It complements, rather than being equivalent to, the CS course on Computer Security (CS 465) and the IT courses on Encryption and Compression (IT 531), Information Assurance and Security (IT 466), and Cyber Security and Penetration Testing (IT 567). This is a 3 credit class. The BYU Catalog states that "The expectation for undergraduate courses is three hours of work per week per credit hour for the average student who is appropriately prepared; much more time may be required to achieve excellence." Thus, an average student should expect to spend at least 6 hours per week outside of lecture on working problems, reading the textbook, reviewing concepts, and completing assignments.

Honor Code: In keeping with the principles of the BYU Honor Code, you are expected to be honest in all of your academic work. Academic honesty means, most fundamentally, that **any work you present as your own must in fact be your own work and not that of another**. Violations of this principle may result in a failing grade in the course and additional disciplinary action by the university. You are also expected to adhere to the Dress and Grooming Standards. It is the university's expectation, and my own expectation in class, that you will abide by all Honor Code standards. Please call the Honor Code Office (4440 WSC) at 801-422-2847 if you have questions about those standards.

Preventing Sexual Harassment: Title IX of the Education Amendments of 1972 prohibits sex discrimination against any participant in an educational program or activity that receives federal funds. The act is intended to eliminate sex discrimination in education and pertains to admissions, academic and athletic programs, and university-sponsored activities. Title IX also prohibits sexual harassment of students by university employees, other students, and visitors to campus. If you encounter sexual harassment or gender-based discrimination, please talk to your professor, contact the Equal Employment Office at 801-422-5895 or 1-888-238-1062 (24 hours) or http://www.ethicspoint.com, or contact the Honor Code Office (4440 WSC) at 801-422-2847.

Students with Disabilities: BYU is committed to providing reasonable accommodation to qualified persons with disabilities. If you have any disability that may adversely affect your success in this course, please contact the University Accessibility Center office (2170 WSC) at 422-2767. Services deemed appropriate will be coordinated with the student and instructor by that office.

Crypto-challenge

At the start of the semester, the class will be divided into teams. Each student and each team will be given a "secret" (a large number in hexadecimal form), which will be used in various assignments, with the result posted to a Digital Dialog discussion board. Despite this, your personal secret itself should not be shared with any other student (including teammates), and your team secret should not be shared with other teams.

Over the course of the semester there will be a competition for both teams and individuals. Participation (or lack thereof) will not impact your grade directly, but you may find the extra practice will help you master the material. There will also be prizes for the victors. Points towards the competition may be earned by

- Carrying out bonus assignments,
- Cracking secret messages I may leave in the homework, online or elsewhere,
- Successfully cracking encrypted messages posted by other students or teams as part of certain assignments,
- Discovering another student's or team's secret,
- At my discretion for exceptional work or ideas.

Unlike homework solutions, challenge secrets may be shared, traded, bartered, or spilt on Digital Dialog.

Points may be claimed by emailing the solution to me, along with an explanation of how you obtained it, **before the secret is spilt on the discussion board**. If your personal or team secret gets out, you will lose points per person or team who claims your secret. If your secret is spilt online, you or your team will be out of the individual or team competition entirely. Therefore, for assignments which require you to use your secret and post a result to the discussion board, it is vital that you do so carefully and not leave your secret vulnerable to exploits.

The challenge ends and victors will be awarded at the scheduled final exam time.

A X Y D L B A A X R
is L O N G F E L L O W

One letter stands for another. In this sample, A is used for the three L's, X for the two O's, etc. Single letters, apostrophes, the length and formation of the words are all hints. Each day the code letters are different.

9-6 CRYPTOQUOTE

T YIKQ JISA ABNVPQZ YBLQ

VQQU ZEQQM, BUF JISA

AQLQATQZ ZKBRTISZ.

— QNTPJ FTRDTUZIU

Yesterday's Cryptoquote: BY ALL THESE LOVELY TOKENS, SEPTEMBER DAYS ARE HERE, WITH SUMMER'S BEST OF WEATHER AND AUTUMN'S BEST OF CHEER. — H.H. JACKSON