Math 485: Section 001, Fall 2018
MWF 1:00 – 1:50, 116 TMCB

Instructor: Rod Forcade – 316 TMCB
   Email: forcader@math.byu.edu
   Web: http://www.math.byu.edu/~forcader/m485F18.html
   Phone: 801-422-2379 (extension 22379 on campus)
   Office Hours: TBA

TA: Dongsheng Wu – 330 TMCB
   Office Hours: TuTh 2-3

Text: Introduction to Cryptography with Coding Theory (2nd ed.)
   by Trappe and Washington.

Prerequisites: Math 313. Math 371 is helpful, but not required. (Chapter 3 of our
text will cover most of what’s needed in that vein.) A little programming
experience is also helpful, but there are Mathematica and Maple examples in the
back of the book, and we’ll use sage, which is easy to learn (and free).

Scope of the Course: This course is designed to cover primarily the mathematical side
of modern cryptography, so we’ll be less interested in the details of programming – but it’s fun to
learn how the average student, with just a laptop, can devise a personal cryptosystem which is
virtually unbreakable (within the lifetime of the universe). Surprisingly, it’s the ordinary math
stuff (factoring, exponentiating, etc.) which make it all possible.

We’ll start with symmetric codes (substitution ciphers, block ciphers, DES, etc). Then we’ll do a
little number theory (which underlies most modern cryptography) including Euclid’s algorithm,
modular arithmetic and exponentiation, Fermat and Euler theorems, primitive roots, elementary
continued fractions and a brief venture into finite fields. We’ll learn about public-key (non
symmetric) cryptography, including knapsack and especially RSA (which you have probably
used without knowing it) and we’ll explore its strengths and weaknesses. That will lead to a
discussion of primality testing and factorization techniques (e.g. the Quadratic Sieve). We may
also look at elliptic curve cryptography, since it’s a wonderful application of geometry to code-
making.

Grading: Homework (including codes to make and break) will be assigned in each class and
collected in the following class. A partial assignment list will be available by the end of the first
week. There will also be two tests (to be announced) and a final. Homework will be 30% of
your grade, mid-terms will be 20% each, and the final will be another 30% of your grade.
Grades will be A:95-100%, A-:90-94%, B+:87-89%, B:83-86%, B-:80-82&+, etc. Under 60% is failing.

---------------------------------------------------------------------------------

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 at 801-422-2847.

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 at 422-2767. Services deemed appropriate will be coordinated with the student and instructor by that office.