Number Theory & Mathematical Cryptography

(Two previous versions of [Spring 2013] and [Spring 2011] NT&MC have nice photos of the class.)

MAT4930 2H22 : *NT&Math-Crypto counts as an Upper-division math-elective.*

This is a 1-semester course for folks interested in Mathematical Cryptography (major topic) and other aspects of *Coding*: Data Compression and (*time permitting*) Error-correcting codes. We will also cover one example of an Isomorphism code.

It is accessible to anyone with an introductory NT course or who has read the first chapter or two of a beginning NT text.

(I'd like you to know *What a prime number is*, and *What mathematical induction is* and *What an equivalence relation is*. Also helpful is how to "add two numbers mod N", and what the Euler phi function is.)

Good choices [all these books are in Marston Science Library, on campus] for self-study are:

- *Elementary Number Theory* by James Strayer; *or*
- *A Friendly Introduction Number Theory* by Joseph Silverman; *or*
- *Elementary Number Theory* by David Burton; *or*
- the text by Vanden Eynden.

Our Teaching Page has useful information for students in all of my classes. It has **my schedule**, LOR guidelines, and Usually Useful Pamphlets. One of them is the *Checklist* (pdf) which gives pointers on what I consider to be good mathematical writing. Further information is at our class-archive URL (I email this private URL directly to students).

We'll have a **test of prerequisite knowledge** on Friday, 08Jan2016.

The mini-test counts for little, about 2%—4% of course grade, and selects *some* topics from:
:: *High-school knowledge* (formula for a line between two points, the Quadratic Formula, intersecting a line with a parabola, etc.), and some
:: *Sets&Logic ideas* (Equivalence relations, partial orders, binary operators, induction, pigeon-hole principle, cardinality, powerset operator, etc.)
:: *Mathematical maturity* (Do you remember your basis calculus stuff? Do you remember how to sum a geometric series?)
The :: Math-Greek alphabet (pdf), which we will use in class frequently.
Available is a practice prereq.

Resources from a previous incarnation of the course

- My Notes on Codes (pdf).
- xkcd Cryptography
- A topics guide (txt) for one of the exams.
- For the curious, Huffman's original 1952 paper (pdf).
- Empirical Entropy of English. (Claude Shannon's experiment); needs Java enabled, to run.

Approx. Syllabus

- A review of modular arithmetic.
- Versions of The Euclidean Algorithm (the "Lightning Bolt" alg).
  - *Possibly*: LBolt over the Gaussian Integers. Proving unique factorization in the Gaussian Integers. Using LBolt to write certain primes as sums-of-two-squares.
  - Euler phi function, Fermat's Little Thm. Euler-Fermat Thm (EFT). The Legendre and Jacobi symbols.
  - The RSA Cryptosystem.
  - The Chinese Remainder Thm (CRT) and a brief introduction to Rings and Ring-isomorphism.
- Huffman codes. Huffman's theorem on *minimum expected coding-length* codes. Uniquely-decodable codes and the Kraft-McMillan theorem.
  - Elias delta code and the Ziv-Lempel adaptive code.
  - Diffie-Hellman Cryptosystem. Shank's *Baby-step Giant-step* method for trying to break the Diffie-Hellman protocol.
  - Pollard-ρ factorization algorithm. *Descent-from-the-Top* algorithm for computing the mod-*M* mult. order of an element.
  - *Possibly*: Pollard's *p-1* factorization algorithm.
  - Miller-Rabin algorithm. Possibly: Polytime testing whether *N* is a prime-power.
- Multiplicative functions. Dirichlet convolution.
  - *Possibly*: Along the way to developing cryptographic methods, we will solve a number of Diophantine equations, that is, algebraic equations where the only solutions that we allow are using integers. We will find all "Pythagorean triples" (a,b,c) of positive integers for which

    $a^2 + b^2 = c^2$.

    We will discover that there is a two-parameter family of such solutions. See "Pythagorean Triples (pdf)" at Usually Useful Pamphlets.
  - *Possibly*: Meshalkin Isomorphism code.

```
 ENCODING:
a  b  c  d  e  f  g  h  i  j  k  l  m  n  o  p  q  r  s  t  u  v  w  x  y  z     '  .  ?  !  ,
0  1  2  3  4  5  6  7  8  9 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24 25 26 27 28 29 30 31
```

Three Examples of simple ciphers:

```
 CAESAR: Shift of 9:
a  b  c  d  e  f  g  h  i  j  k  l  m  n  o  p  q  r  s  t  u  v  w  x  y  z     '  .  ?  !  ,
9 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24 25 26 27 28 29 30 31  0  1  2  3  4  5  6  7  8

 MULTIPLICATIVE-CIPHER: Mult by 5:
a  b  c  d  e  f  g  h  i  j  k  l  m  n  o  p  q  r  s  t  u  v  w  x  y  z     '  .  ?  !  ,
0  5 10 15 20 25 30  3  8 13 18 23 28  1  6 11 16 21 26 31  4  9 14 19 24 29  2  7 12 17 22 27

 AFFINE-CIPHER: Mult by 5, then add 9.  x |-> [5*x]+9 (mod 32)
a  b  c  d  e  f  g  h  i  j  k  l  m  n  o  p  q  r  s  t  u  v  w  x  y  z     '  .  ?  !  ,
9 14 19 24 29  2  7 12 17 22 27  0  5 10 15 20 25 30  3  8 13 18 23 28  1  6 11 16 21 26 31  4
```

Various math czars who help out.

Chalk	Phone	Time	Computer/Proj	Blackboard	Humor	E-Problems

Resources on "The Web"

א. If she saw this, (TAotDM), WWSKnow?

ב. The decipherment of a substitution cipher appears in The Gold Bug, by Edgar Allan Poe.

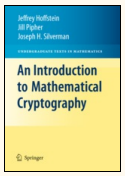
ג. Wikipedia. See also Primality testing and links to original AKS article and improvement.

ד. Historical Cryptography (Trinity College)>.

ה. MathPages. (I haven't reviewed this.)

ו. Sample chapters from the Handbook of Applied Cryptography. (I have not reviewed this book.)

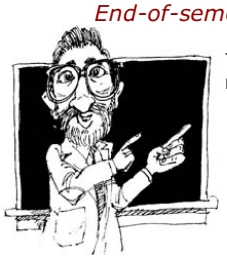
Our textbook is *An Introduction to Mathematical Cryptography* (*Undergraduate Texts in Mathematics*).



Authors: Jeffrey Hoffstein, Jill Pipher, J.H. Silverman
ISBN: 978-0-387-77993-5
Year: 2008
Publisher: Springer
Marston: QA268 .H64 2008
Electronic: Chap. 1 and Chap. 2, Diffie-Hellman, etc. (Free for UF students)

The homepage of ... *Mathematical Cryptography*, with a link to its Errata sheet.
Here are links to this book at The Publisher's site and at Amazon.com.

End-of-semester NT Individual project



The Individual Final Project will be due, slid under my office door (Little Hall 402, Northeast corner), no later than **noon, Thursday, 21Apr2016**.

*The project must be **carefully typed***, but diagrams may be hand-drawn.

At all times have a **paper copy** you can hand-in; I do ***NOT*** accept electronic versions. Print out a copy *each day*, so that you *always* have the latest version to hand-in; this, in case your printer or computer fails. (You are too old for "My dog ate my homework.")
Please follow the guidelines on the *Checklist* (pdf, 3pages) to earn full credit.

JK Home page

____End: Number Theory