ADVANCED CRYPTOLOGY (COD2)

CTY COURSE SYLLABUS

Week 1

Info sheet, pre-test, Sunday survey, honor codes, computer lab forms, check roster

Day 1

morning

- "Previously … in Cryptology": skit
- Introductions
- Icebreaker involving modular arithmetic
- Classroom rules
- The map of CODE on the board

afternoon

- CODE map continued
- Re: cipher wheels & how to do Caesar and Vigenère on TI with his program WHEEL
- auto-key encryption

evening

- worksheet #1 on icebreaker and use of WHEEL, auto-key
- Reviewing with course pack

Day 2

morning

- Review of the Euclidean Algorithm
- Review of the EEA
- Multiplicative inverses in mods

afternoon

- Review of public-key cryptography and authentication
- Knapsack ciphers

- Motivation of and introduction to matrices

evening

- Worksheet. Heavy on a knapsack exchange and a problem illustrating why 2 x 2 matrices multiply the way they do.

Day 3

morning

- More on matrices, up to and including inverses and how to do everything on the calculator.
- Error-correcting codes. Motivation of the generator matrix.

afternoon

- More ECC, writing down the steps and getting the students to do it
- Permutations: cycle notation, composition, identity, inverses
- Intro to McEliece encryption, up to definition and calculation of public key F

evening

- Day three worksheet.

Day 4

morning

- McEliece public key encryption

afternoon

- More McEliece stuff.
- Fermat skit
- Factoring vs. primality testing as mathematics problems
- Fermat Factorization

evening

- Day 4 Worksheet

Day 5

morning

- COD2 Map – summary of what we've learned so far in COD2, and calculator program sharing
- Computer lab: Looking at multiplication tables and exponent tables and making conjectures and seeing the connection to cryptology

afternoon

- More time finishing up the lab
- Discussion of what was learned in the lab
- The square-multiply method
- Sideshow: Intro to probability and statistics applied to crypto, up through basic addition and multiplication rules.

evening

- (Sunday) Worksheet on mods stuff (bring up primitive roots)

Week 2

Day 6

morning

- More probability, derangements
- Cracking codes using statistics – the index of coincidence

afternoon

- Pollard rho factorization
- Review of Diffie-Hellman and RSA

evening

- Work on Simon Singh challenge, worksheet

Day 7

morning

- ElGamal encryption

- The Pollard-(p-1) method of factorization

afternoon

- Digital signatures and ElGamal applied thereto

evening

- Constructing new Enigma machines, worksheet

Day 8

morning

- Primality testing
- Permutations and their application to the Enigma

afternoon

- Carmichael numbers, the Miller-Rabin Primality Test
- Euler's Phi function
- Intro to Enigma rotor recovery problem

evening

- Study for midterm

Day 9

morning

- The midterm exam

afternoon

- Review of the midterm
- Completion of second Enigma unit.

evening

- Completion of second Enigma unit, exercises.

Day 10

morning

- M-209: The introduction – history, how it works, encrypting/decrypting on paper.

afternoon

- elective topics: pseudo-random numbers and authentication challenges? P vs. NP complexity issues in mathematics/crypto?
- M-209 training video from the 1950's

evening

- Special lecture in Adams Auditorium with Number Theory and Math Reasoning classes

Week 3

Day 11

morning

- Extensive history of science and our understanding of the world
- Our current understanding of the universe and quantum mechanics
- Quantum computing

afternoon

- Quantum computing demo
- M-209 – more about the mathematics underlying the machine

evening

- Exercises

Day 12

morning

- The M-209: encrypting "manually," and the protocol for its use.
- The M-209 crack part I: cribbing

afternoon

- Quadratic sieve

- The M-209 crack part II: just beginning

evening

- Exercises related to the day

Day 13

morning

- M-209 Crack Part II and III: finding relative settings of pins on rotors and the cage, discussion of finishing off the crack
- Continued fractions

afternoon

- Mathematics needed to understand elliptic curves

evening

- study for final, work on Simon Singh challenge

Day 14

morning

- Elliptic curve cryptology

afternoon

- Final Exam Part I: cracking the Kryha machine

evening

- Final Exam Part II: cracking the Kryha machine

Day 15

morning

- Post-assessment test given