Number Theory & Mathematical Cryptography: Syllabus

S2014: MAT4930 7554 Number Thy & Cryptography MWF6 LIT221

Office: 402 Little Hall (Top floor, NE corner, “Maximize x, y and z.”)

Telephone: *352-294-2314*. If I am not in the office then it is best to

EMAIL me at the **squash@ufl.edu** eddress.

If urgent then telephone to the Math Office at

352-392-0281.x221 and they can contact me at home.

OFFICE HOURS: Currently Mondays and Wednesdays 8th period [15:00-15:50].

I am also available for APPOINTMENT, especially on Mon. or Wedn., 9th [16:05-16:55].

My OHs will >>VARY<< during the semester; I will announce changes.

ARCHIVE: You and I will post/read Solutions to problems, at our Class Archive.

To *view* the Archive, point a browser at

https://lists.ufl.edu/cgi-bin/wa?A0=NUMT-L

To *post* to the Archive, email to eddress NUMT-L@lists.ufl.edu

/from/ your UF eddress.

PREREQUISITE: General NT knowledge: Modular-arithmetic, Euler-phi fnc, Chinese

Rem. Thm., basic prime numbers. Also assumes basic calculus, and proof techniques

[e.g, mathematical induction] from Sets&Logic (MHF3202) or Numbers&Polynomials

(MAS3300). /Helpful/, but not required: Knowledge of the math-Greek alphabet. A

Linear Algebra course.

There be 2 take-home exams (done in teams), with an in-class component (done

individually); the score is approx. 250+140=290points for each exam.

Instead of a final exam, there is an Individual-project, due 11:30AM, due Friday,

25Apr2014. The project, and the take-home exams, must be carefully typed.

There will be a number of pop-quizzes, each counting 30points. You get 5points

for free, simply for attempting the pop-quiz, as this encourages folks to be in

class

My course has a SUBSTANTIAL class-participation grade, and attendance is REQUIRED.

My course has a SUBSTANTIAL class-participation grade, and attendance is REQUIRED.

HOMEWORK: I'll ask that you post your homework to the Archive, so that we can get intelligent comments from many minds. I give a CP (class participation) grade each month, approx. 45points, based on Posting, Speaking in class, Speaking with me outside of class, and helping your classmates, e.g, lending notes, working at the blackboard with other students.

GRADES: During the week before the withdraw date, *Friday, 11Apr2014*, I give you a ***written estimate*** of your course letter-grade.

CLASS-PHOTO DAY: Wednesday, 15Jan2014. Look sharp! Please bring name-card with (optional but useful) your telephone number.

Letters-of-recommendation (LORs): I base LOR substantially on how a student "thinks on his feet". I require have had /two/ courses with me before asking for a LOR. See my Teaching Page for important details.

Potential topics: Our webpage has a list; here is a partial list:
Huffman codes. Huffman's theorem on Minimum Expected Coding-Length codes.
Diffie-Hellman Cryptosystem. Shank's Baby-step Giant-step method for trying to break the Diffie-Hellman protocol.
RSA Cryptosystem.
Miller-Rabin algorithm. Also, polytime testing whether N is a prime-power.
Pollard's p-1 and rho factorization algorithms.
Smith Normal Form of a matrix to solve a system of linear Diophantine equations.
Review: Euclidean Algorithm (the Lightning Bolt alg). Also over the Gaussian Integers. Proving unique factorization in the Gaussian Integers.
Using Lightning Bolt to write certain primes as sums-of-two-squares.
Euler phi function, Fermat's Little Thm.
The Chinese Remainder Thm and a brief introduction to Rings and Ring-isomorphism.
The Legendre and Jacobi symbols.