Math 116: General Course Outline

Catalog Description

116. Mathematical Cryptology. (4) Lecture, three hours; discussion, one hour. Requisite: course 115A. Not open for credit to students with credit for Program in Computing 130. Introduction to mathematical cryptology using methods of number theory, algebra, probability. Topics include symmetric and public-key cryptosystems, one-way functions, signatures, key exchange, groups, primes, pseudoprimes, primality tests, quadratic reciprocity, factoring, rho method, RSA, discrete logs. P/NP or letter grading.

Textbook

Trappe, *Intro to Cryptography with Coding Theory*, Prentice Hall.

Reviews & Exams

The course is planned for 28 lectures, 1 midterm exam, and 1 holiday.

Schedule of Lectures

Week	Section	Topics
1	1.1-1.4, 2.1-2.2	Congruences, Classic Symmetric Ciphers, Intro to Probability. Read: Introduction, 1.1-1.4, 2.1-2.2.
2	2.3-2.4, 4.4, 3.1-3.5	Probability (cont.), Applications to Attacks, Permutations. Read: 2.3-2.4, 4.4, 3.1-3.5.
3	4.1-4.2, 6.1-6.3, 7.1-7.2	Symmetric Ciphers (Vigenere, DES, AES), Theory of Integers (Factorization, GCD, Euclidean Algorithm). Read: 4.1-4.2, 6.1-6.3, handout on AES (Rijndael), 7.1-7.2.
4	7.3-7.8, 8.1-8.2	Theory of Integers (Euclidean Algorithm, Equivalence Relations, Integers mod n, Discrete logs, Primitive roots, Linear Algebra mod n), affine cipher. Read: 7.3-7.8, 8.1-8.2.
5	10.1-10.5	Public Key Ciphers (RSA, Diffie-Hellman, ElGameal, Knapsack). Read 10.1-10.5.
6	12.1-12.6	**Midterm Monday.** Roots mod p. Read: 12.1-12.5.
7	13.1-13.3, 13.5-13.7, 15.1-15.5	Roots mod n, Quadratic Reciprocity. Read: 13.1-13.3, 13.5-13.7, 15.1-15.5.
8	16.1-16.6	Pseudo-primes and Primality tests, Prime Generation. Read: 16.1-16.6.
9	24.1-24.3	Factorization Attacks. Read: 24.1-24.3.
10	27.1-27.3	Discrete logs, Review. Read: 27.1-27.3.

Comments

Outline update: D. Blasius, 2/02

NOTE: While this outline includes only one midterm, it is strongly recommended that the instructor considers giving two. It is difficult to schedule a second midterm late in the quarter if it was not announced at the beginning of the course.

For more information, please contact Student Services, ugrad@math.ucla.edu.