Math 135: The Art of Secret Writing (Summer 2006)
Syllabus

The following references are to the textbook *Invitation to Cryptology* by Thomas H. Barr.

June 26	Introduction to Cryptography/Cryptology	§1.3, §1.1
June 27	Crypto-Chronology	§1.1
June 28	Functions	§1.2
June 29	Shift Ciphers/Modular Arithmetic	§2.1
June 30	Shift Ciphers (cont.); Affine Ciphers	§2.1, §2.2
July 3	Affine Ciphers/Multiplicative Inverses	§2.2
July 4	NO CLASS	
July 5	Substitution Ciphers	§2.3
July 6	Transposition Ciphers	§2.4
July 7	Review §1.1 – §2.4	
July 10	Prelim #1	
July 11	Polyalphabetic Ciphers	§2.5
July 12	Probability	§2.6
July 13	Probability (cont.); Friedman and Kasiski Tests	§2.6, §2.7
July 14	Hill Cipher; Matrices	§2.9
July 17	Hill Cipher; Matrices (cont.)	§2.9
July 18	Number Representation	§3.1
July 19	Boolean and Numerical Functions	§3.2
July 20	Computational Complexity	§3.3
July 21	Review §2.5 – §3.3	
July 24	Prelim #2	
July 25	Introduction to Public Key Crytography and PGP	pages 243, 264–265, §5.2
July 26	Primes and Prime Factorization	§4.1
July 27	Euclidean Algorithm	§4.1
July 28	Fermat's Little Theorem	§4.3
July 31	RSA Public Key Cryptosystem	§4.4
August 1	RSA (cont.); Public Key Infrastructure	§4.4, §5.3
August 2	Key Agreement	§5.4
August 3	Digital Signatures; Law and Cryptography	§4.6, §5.4
August 4	Final Exam Review	
August 8	FINAL EXAM (8:00 – 10:00 a.m. in Malott 206)	