Mathematics 124 (Winter 2009)
Syllabus

Tuesday, January 6	Introduction to Cryptography/Cryptology	§1.3, §1.1
Thursday, January 8	A Crypto-Chronology (Part I)	§1.1
Tuesday, January 13	A Crypto-Chronology (Part II)	§1.1
Thursday, January 15	Functions	§1.2
Tuesday, January 20	Modular Arithmetic	§2.1
Thursday, January 22	More Modular Arithmetic, Affine Ciphers	§2.2
Tuesday, January 27	Substitution Ciphers, Transposition Ciphers	§2.3, §2.4
Thursday, January 29	The Vigenère Keyword Cipher	§2.5
Tuesday, February 3	Probability and Expectation (Part I)	§2.6
Thursday, February 5	Probability and Expectation (Part II)	§2.6
Tuesday, February 10	The Friedman and Kasiski Tests	§2.7
Thursday, February 12	Matrices and the Hill Cipher	§2.9
Tuesday, February 17	NO CLASS (UNIVERSITY HOLIDAY)	
Thursday, February 19	NO CLASS (UNIVERSITY HOLIDAY)	
Tuesday, February 24	The Hill Cipher	§2.9
Thursday, February 26	Number Representation	§3.1
Tuesday, March 3	Binary One-Time Pad	§3.4
Thursday, March 5*	Feedback Shift Registers (*meet in ED 314)	§3.4
Tuesday, March 10	Introduction to RSA and Public Key Cryptography	pages 243, 264–265, §5.2
Thursday, March 12	Prime Numbers	§4.1
Tuesday, March 17	To Be Announced	
Thursday, March 19	MIDTERM	
Tuesday, March 24	Euclidean Algorithm	§4.1
Thursday, March 26	Fermat's Little Theorem	§4.3
Tuesday, March 31	Fermat's Little Theorem	§4.3
Thursday, April 2	The RSA Public Key Cryptosystem	§4.4
Tuesday, April 7	Basic Internet Security	Notes
Thursday, April 9	The Diffie-Hellman Key Agreement Protocol	§4.5
Tuesday, April 21	FINAL EXAM (14:00 – 17:00)	