MATH 314
Introduction to Cryptography (3 units)

Course Outline

Chapter(s)	Topics	# of weeks
1	**Overview of Cryptography and Cryptanalysis** Kerchoff's Principle; Types of attacks, and cryptographic applications.	0.5
2	**Classical Cryptography** Caesar, Vigenere and Hill ciphers; Cryptanalysis of classical ciphers; the one-time-pad and perfect secrecy.	2
3	**Elementary Number Theory** Modular arithmetic; Euclid's Algorithm; Chinese Remainder Theorem; Fermats Little Theorem and Eulers Theorem; Modular Exponentiation; 3-Pass-Protocol; Primitive Roots; Legendre and Jacobi Symbols; Finite Fields.	3.5
4-5	**Modern Symmetric Key Cryptography** Feistel Ciphers; SDES and DES; Differential Cryptanalysis; 2DES and Meet-in-the-middle attacks; 3DES; AES/SAES.	3.0
6-7	**Public Key Cryptography** RSA; The Fermat, Miller-Rabin and Solovay-Strassen primality tests; Factoring, Dixon's Factorization Algorithm; Discrete logarithms, Diffie-Hellman key exchange, ElGamal.	2.5
8-9	**Hash Functions and Digital Signatures** Hash Functions; Collisions and Collision resistance, Birthday attacks, RSA and other signature algorithms.	1.5
10–16	**Further Topics (as time permits)** Security Protocols; Digital Cash; Zero Knowledge Techniques; Elliptic Curves Cryptography; Error Correcting Codes; Quantum Cryptography.	
	Tests	1.0

Textbook: *Introduction to Cryptography*, 2nd edition, by Wade Trappe and Lawrence Washington.

Adopted: Spring 2018.