Pries: 360 Mathematics of Information Security: Fall 2019 Tentative Syllabus

Week	Starts	Topics
		Introduction to number theory and public key cryptography
1	8/26	Ciphers, Euclidean algorithm, modular arithmetic
2	9/4	Fermat's Little Theorem, Primitive roots
3	9/9	Discrete log problem and El Gamal cryptosystem
4	9/16	Euler phi function and RSA cryptosystem
5	9/23	Monday, midterm 1. Sun Ze (Chinese remainder) theorem
		Computation and attacks
6	9/30	Computer lab
7	10/7	Computer lab
8	10/14	primality testing and Pollard's $p-1$ factorization algorithm
9	10/21	Squares and square roots
10	10/28	Rabin encryption, probabilistic encryption
		Refinements, probability, and finite fields
11	11/4	Monday, midterm 2. Miller-Rabin
12	11/11	Zero knowledge proofs
13	11/18	Collision algorithms
		Fall break
14	12/2	Finite fields
15	12/9	Finite fields