Pries M360 - Mathematics of Information Security Fall 2024

This syllabus schedule is tentative!

Week	Starts	Topics
		Introduction to number theory and public key cryptography
1	8/19	Affine ciphers, modular arithmetic
2	8/26	Euclidean algorithm, units
		Discrete Log Problem, Diffie-Hellman, El Gamal
3	9/2	fast exponentiation, Fermat's Little Theorem
4	9/9	order and primitive roots
5	9/16	public key cryptosystems and Diffie-Hellman key exchange
6	9/23	Discrete log problem and El Gamal cryptosystem
		RSA cryptosystem
7	9/30	Sun Ze (Chinese remainder) theorem, Euler phi function, Euler's Theorem
8	10/7	RSA cryptosystem
		Attacks on public key cryptography
9	10/14	Primes and primality testing, Miller-Rabin
10	10/21	Attacks on RSA: Pollard's $p-1$ factorization algorithm
11	10/28	Collision algorithms: baby-step/giant step, attacks on El Gamal
12	11/4	Projects
		Math used in more advanced cryptosystems
13	11/11	Finite fields
14	11/18	Lattice-based cryptography
		Fall break
15	12/2	Review

In-class quiz dates:
Week 2: Fri 8/30; quiz 1
Week 4: Fri 9/13; quiz 2
Week 6: Fri 9/27; quiz 3
Week 8: Fri 10/11; quiz 4
Week 10: Fri 10/25; quiz 5
Week 12: Fri 11/08; project due
Week 14: Fri 11/22; quiz 6
Final exam: Tuesday Dec 10, 11:50 am - 1:50 pm.

Grading scheme:
15% in-class participation; (class attendance mandatory)
15% homework
30% in-class quizzes (5% each);
15% cryptography project;
25% final.