Math 173A Suggested Syllabus

Text: *An Introduction to Mathematical Cryptography,* J. Hoffstein, J. Pipher, and J. Silverman

Lecture	Section	Topic
1	1.1	Overview, Simple substitution ciphers
2	1.2	Divisibility and greatest common divisors
3	1.3	Modular arithmetic
4	1.3	Modular arithmetic (continued)
5	1.4	Prime numbers, unique factorization, and finite fields
6	1.5	Powers and primitive roots in finite fields
7	1.7	Symmetric and asymmetric ciphers
8	2.1	The birth of public key cryptography
9	2.2	The discrete logarithm problem
10	2.3	Diffie–Hellman key exchange
11	2.4	The ElGamal public key cryptosystem
12	2.6	How hard is the discrete logarithm problem?
13	2.7	A collision algorithm for the DLP
14		Review
15		**Midterm**
16	3.1	Euler's formula and roots modulo pq
17	3.2	The RSA public key cryptosystem
18	3.3	Implementation and security issues
19	3.4	Primality testing
20	3.5	Pollard's $p-1$ factorization algorithm
21	3.5	Pollard's $p-1$ factorization algorithm (continued)
22	3.6	Factorization via difference of squares
23	3.6	Factorization via difference of squares (continued)
24	3.7	Smooth numbers and sieves
25	3.7	Smooth numbers and sieves (continued)
26	3.8	The index calculus and discrete logarithms
27	3.9	Quadratic residues and quadratic reciprocity
28		Review 1
29		Review 2