Math 5248, Fall 2004

1. Simple ciphers: homework due Wed Sept 15
   - shift cipher, reduction/division algorithm, one-time pad, affine cipher
   - multiplicative inverses mod 26

2. Counting and Probability: homework due Wed Sept 22
   - Sets, functions, counting, statistics of English

3. Permutations: homework due Wed Sept 29
   - Cryptograms, anagrams, permutations, shuffles, interleavers

4. Vigenere Cipher, more probability: homework due Wed Oct 6
   - LCMs and GCDs, Expected Values, Friedman Attack, Generating Functions,
   - Variance, Law of Large Numbers

Supplement: DES and AES: lectures Wed Oct 6 through Mon Oct 11
   - Modern Symmetric Ciphers, Design Goals,
   - Data Encryption Standard, Advanced Encryption Standard

Midterm I: Wed Oct 13

5. Integers: homework due Wed Oct 20
   - Divisibility, primes, unique factorization, Euclidean Algorithm,
   - multiplicative inverses, computing inverses

   - Integers mod m, square-and-multiply, primitive roots, discrete logs, algebraic identities

7. Integers (continued): homework due Wed Nov 3
   - Fermat’s little theorem, square roots, cube roots

Supplement: Primes: Wed Nov 3 through Mon Nov 8
   - Euclid’s Theorem, Prime Number Theorem, Riemann Hypothesis

Supplement: Groups and rings: Wed Nov 3 through Mon Nov 8
   - Lagrange’s theorem, universality of $0 \cdot r = 0$, etc.

Midterm II: Wed Nov 10

8. Integers (continued) and intro to PK: homework due Wed Nov 17
   - RSA, Diffie-Hellman key exchange, ElGamal cipher
   - Fermat pseudoprimes, Miller-Rabin and strong pseudoprimes

9. Roots Mod Composites: homework due Wed Nov 24
   - Sun Ze’s Theorem, Euler’s theorem,
   - facts about primitive roots, Hensel’s Lemma, Euler’s Criterion

10. Factorization: homework due Wed Dec 1
    - square-root oracle factoring, Pollard’s rho, Pollard’s $p - 1$
    - random squares, quadratic sieve, primality certificates, Pocklington-Lehmer

Supplement: Protocol sketches: Wed Dec 1 through Mon Dec 6

Midterm III: Wed Dec 8

11. Pseudo Random Number Generators: homework due Wed Dec 15
    - Fake One-Time Pads, period of pRNGs, LCGs, LFSRs, Blum-Blum-Shub, Naor-Reingold, primitive polynomials

Supplement: Quadratic reciprocity: Wed Dec 15