An introduction to the number theory behind computer science with a specific focus on applications in cryptography.

NOTE: Many topics will likely have to be discarded

1. Intro
    a. Background expected: FOCS
2. What is number theory
3. What are the applications of number theory in computer science
    a. Crypto
    b. Error Correction
    c. Random Number Generation
4. Modular Arithmetic
    a. Clock stuff
    b. Why is modular arithmetic important
    c. Ring of integers mod n
    d. When does a modular inverse exist
    e. Field of integers
        i. Finite fields
5. RSA/Diffie hellman
    a. RSA
        i. Euler-Fermat
    b. Diffie Helman
        i. Discrete Log
6. Finding Primes
    a. How many primes are there?
        i. Prime counting function
        ii. Prime number theorem
        iii. Approximations to prime counting theorem
            1. x/log x
            2. Logarithmic integral
    b. Sieve of Eratosthenes
7. Primality Checking
    a. Fermat
    b. Miller-Rabin
    c. Baillie–PSW
8. Factorization
    a. Naive
    b. Pollard p-1
    c. Pollard Rho
    d. General Number Field Sieve
        i. http://www.ams.org/notices/199612/pomerance.pdf

9. Strong primes
10. Elliptic curve
    a. NSIT standard
    b. Nothing up my sleeve numbers
11. Other fun topics
    a. Diophantine equations
        i. Hilbert's 10th problem
    b. Reiman hypothesis
        i. Connection to prime numbers
    c. Fermat’s last theorem