Week	Days	Tuesday	Thursday
1	Jan 12, Jan 14	Welcome, substitution ciphers (Read 1.1)	Gcd, divisors, Euclidean algorithm, Bezout (Read 1.2)
2	Jan 19, Jan 21	Modular arithmetic and Z/mZ (Read 1.3)	Totient function, successive squaring, finite fields (Read 1.4)
3	Jan 26, Jan 28	Finite fields, FLT, runtime estimates (Read 1.5)	DLP, Diffie-Hellman (Read 2.1, 2.2, 2.3)
4	Feb 2, Feb 4	ElGamal (Read 2.4)	Group Theory, (Read 2.5)
5	Feb 9, Feb 11	Baby-Step-Giant-Step (Read 2.6,2.7)	Chinese remainder theorem (Read 2.8)
6	Feb 16, Feb 18	READING	WEEK
7	Feb 23, Feb 25	Pohlig-Hellman (Read 2.9)	Midterm test
8	Mar 2, Mar 4	Roots mod p and RSA (Read 3.1, 3.2)	RSA and Miller-Rabin (Read 3.3, 3.4)
9	Mar 9, Mar 11	Miller-Rabin, Pollard p-1 (Read 3.5)	Difference of squares (Read 3.6)
10	Mar 16, Mar 18	More difference of squares	The index calculus (Read 3.8)
11	Mar 23, Mar 25	More index calculus	Intro to elliptic curves (Read 6.1)
12	Mar 30, April 1	Elliptic curves over finite fields, double- and-add (Read 6.2, 6.3, 2.10)	ECDLP, Diffie-Hellman, ElGamal (Read 6.4)
13	April 6, April 8	ECDLP, Diffie-Hellman, ElGamal (Read 6.4)	Digital Signatures,… (Read 4, 6.4.3)
14	April13, April 15	Review	Final exam(Tentative date)