CTY Course Syllabus
Advanced Cryptology

Day	Time	What (Knowledge, concepts, reading)
WEEK ONE		
Day 1 Monday	Morning	• Pre-Assessment • "Previously … in Cryptology" • Introductions • Icebreaker
	Afternoon	• Error-correcting codes
	Evening	• Singh Challenge 1
Day 2 Tuesday	Morning	• Evening exercises review • Review: public-key cryptography • McEliece Cryptosystem
	Afternoon	• Fermat Factorization
	Evening	• Exercises
Day 3 Wednesday	Morning	• More McEliece cryptosystem
	Afternoon	• Review of Extended Euclidean Algorithm
	Evening	• Modular arithmetic review • Singh Challenge 2
Day 4 Thursday	Morning	• Multiplicative inverses • Fermat primes • Frequency analysis
	Afternoon	• Square-multiply method • Binary • Review of RSA and Diffie-Hellman Key Exchange
Day 5 Friday	Morning	• Exponential tables and primitive roots
	Afternoon	• Pollard-rho factorization
	Evening (Sunday)	• Exercises
WEEK TWO		
Day 6 Monday	Morning	• More Pollard-rho • Introduction to ElGamal • History interlude • Statistical attacks
	Afternoon	• More statistical attacks
	Evening	• Singh Challenge
Day 7 Tuesday	Morning	• Roughness, index of coincidence, alternate Vigenere attack
	Afternoon	• Pollard-(p-1) method
	Evening	• Exercises
Day 8 Wednesday	Morning	• ElGamal digital signatures
	Afternoon	• Primality testing

Day	Time	What (Knowledge, concepts, reading)
	Evening	• Exercises
Day 9 Thursday	Morning	• Review of statistical attack on Vigenere, Singh Challenge 4
	Afternoon	• Carmichael numbers, Miller-Rabin primality • Euler's Phi function
	Evening	• Exercises
Day 10 Friday	Morning	• Mid-term
	Afternoon	• M-209 Introduction • M-209 training video from 1950s
	Evening (Sunday)	• Joint class with Number Theory/Math Logic
WEEK THREE		
Day 11 Monday	Morning	• Midterm review
	Afternoon	• M-209 mathematics
	Evening	• Exercises
Day 12 Tuesday	Morning	• Quantum mechanics/philosophy • Quantum cryptography
	Afternoon	• Quantum computing • M-209 manual encryption
	Evening	• Exercises
Day 13 Wednesday	Morning	• M-209 Crack 1: cribbing • Pseudo-random number generation
	Afternoon	• Quadratic sieve • M-209 Crack 2:
	Evening	• Singh challenge, study for final
Day 14 Thursday	Morning	• M-209 Crack 2/3: pins, rotors, cage • Continued Fractions
	Afternoon	• Kryha
	Evening	• Kryha
Day 15 Friday	Morning	• Additional continued fractions • Finish Kryha • Post-assessment