# CTY Course Syllabus
# Advanced Cryptology

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

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