

Cryptology
CTY Course Syllabus

Week 1:

Day 1: Morning – introduction to cryptography, Classroom Computer #2, combinatorics lecture I: the General Multiplication Rule and probability, cipher wheel construction for Caesar shift ciphers

Afternoon – introduction to general monoalphabetic substitution ciphers and cracking one example with spaces, combinatorics lecture II: permutations

Evening – cracking a monoalph without spaces, homework on combinatorics and functions, read up to page 14 in Singh

Day 2: Morning – finishing the crack of the first monoalph example, divisibility and prime factorization

Afternoon – improving monoalphs, intro to the Vigenère cipher, practice with enciphering and deciphering

Evening – second homework on combinatorics, read pp. 14 – 44, appendices A & C

Day 3: Morning – Caesar shift/Vigenère cipher short competition, cracking the Vigenère cipher completed, one example as a class, the Division Algorithm

Afternoon – cracking the second Vigenère competition, the Euclidean Algorithm

Evening – catch up on homework, read up to p. 100 in Singh

Day 4: Morning – discussion of Vigenère idea, leading up to the one-time pad, work in groups to crack first one-time pad, the extended Euclidean Algorithm

Afternoon – crack another one-time pad, introduction to the Playfair cipher

Evening – homework, read up to p. 124, finish one-time pad from afternoon if necessary

Day 5: Morning – Introduction to modular arithmetic, more of the Playfair cipher, how it works, encrypt/decrypt with a partner

Afternoon – cracking Playfair with a crib

Evening (Sunday) – homework on E.E.A. and more Playfair cracks, beginning the ‘design your own cryptosystem project’

Week 2:

Day 6: Morning – Summary of week 1, the ADFGVX cipher: how it works, decryption exercise, more modular arithmetic: finding multiplicative inverses

Afternoon – Multiplicative inverses homework, cracking the ADFGVX cipher

Evening – homework, more work on cryptosystems, read up to p. 142

Day 7: Morning – The Euler phi function, thinking about Caesar shifts and the Vigenère using modular arithmetic, affine encryption affine encrypt/decrypt, cracking with a crib

Afternoon – Lecture and worksheet on matrices, matrix cryptography

Evening – Work on cryptosystem presentations

Day 8: Morning – Cracking matrix cryptography with a crib, student presentations
Afternoon – cracking matrix cryptography with a crib, matrix cracking exercises, study for midterm
Evening – Study for midterm

Day 9: Morning – The Midterm Exam, function lecture: conjugation.
Afternoon – Function lecture V: cycle structure invariance under conjugation, intro to the Enigma lecture
Evening – construction of paper Enigma machines, encrypt/decrypt in pairs, observations of Enigma intercepts

Day 10: Morning – Cracking the Enigma, a full crack of an Enigma message as a class, one in groups
Afternoon – Enigma crack in groups finished
Evening (Sunday) – binary and the Baudot code, lecture on Linear Shift Registers

Week 3:

Day 11: Morning – Field trip to the National Cryptologic Museum
Afternoon – Field trip to the National Cryptologic Museum
Evening – Lecture on mini-DES and block ciphers, read the rest of Singh

Day 12: Morning – Lecture on the square-multiply method, Fermat's Little Theorem, Euler's Theorem
Afternoon – Diffie-Hellman key exchange
Evening – homework, read the rest of Singh

Day 13: Morning – RSA, hashing algorithms
Afternoon – Use of hashing in password protection, digital signatures
Evening – Study for final exam

Day 14: Morning – Final exam, part I
Afternoon – Final exam, part II
Evening – Final exam, part III

Day 15: Morning – *Sneakers* and party