

Cryptology (CODE) CTY Course Syllabus

WEEK ONE			
Day	Time	What (knowledge goals/concepts/reading)	How (activities)
DAY 1 Monday	morning	Honor code, course guidelines Introductions Caesar cipher	Encrypted honor “code,” discussion of what should appear on honor code Icebreaker with students’ names encrypted Construction of cipher wheels, message exchange, individual cipher crack
	afternoon	Monoalphabetic substitution with spaces Combinatorics	Discussion, cipher crack as class, in groups Lecture, Handout
	evening	Combinatorics History of cryptology, monoalphabetic substitution ciphers Practice cracking ciphers	Hand in exercises from handout Read <i>The Code Book</i> , pp. 1-14, appendices A-C “Cruel and unusual” ciphers
DAY 2 Tuesday	morning	Monoalphabetic substitution without spaces, frequency analysis Functions	Cipher crack as class, in groups Lecture, handout
	afternoon	Introduction to polyalphabetic ciphers Vigenère cipher Factorization & the GCD	Discussion Message exchange Lecture
	evening	Functions History of monoalphabetic substitution cipher, frequency analysis Practice cracking ciphers	Hand in exercises Read <i>The Code Book</i> , pp. 14-44 Finish cipher cracks from class, continue “Cruel and unusual” ciphers

Day	Time	What (knowledge goals/concepts/reading)	How (activities)
DAY 3 Wednesday	morning	Practice with Vigenère decryption Vigenère crack, Babbage-Kasiski method Divisibility, division with remainder	Individual decryption competition Cipher crack as class Lecture, handout
	afternoon	Continue Vigenère crack Functions II Introduction to One-Time Pad	Cipher crack in groups Lecture, Handout, discuss exercises in class Discussion, lecture
	evening	Complete Vigenère cracks History of polyalphabetic ciphers	 Read <i>The Code Book</i> , pp. 45-99
DAY 4 Thursday	morning	Repeated-use one-time pad crack, cribbing Euclidean Algorithm	Cipher crack as class Lecture, Handout
	afternoon	Modular Arithmetic I Repeated-use one-time pad crack, key exhaustion	Lecture, handout Cipher crack as class
	evening	Euclidean Algorithm, Modular Arithmetic Complete repeated-use one-time pad crack Cryptography and linguistics	Hand in exercises Complete cipher crack in groups Read <i>The Code Book</i>
DAY 5 Friday	morning	Introduction to polygraphic ciphers, Playfair cipher Extended Euclidean Algorithm, solving Linear Diophantine Equations	Lecture, Message exchange Lecture, handout
	afternoon	Playfair crack Modular Arithmetic II	Cipher crack as class, individually Lecture, handout

WEEK TWO

Day	Time	What (knowledge goals/concepts/reading)	How (activities)
Sunday	evening	Playfair encryption/crack	Finish cipher cracks from class
		Extended Euclidean Algorithm	Hand in exercises
		Modular Arithmetic II	Hand in exercises
		Create your own cryptosystem	Students work on cryptosystems
DAY 6 Monday	morning	Introduction to ADFGVX cipher	Lecture
	afternoon	Cracking the ADFGVX cipher	Cipher crack as class, in groups
		Mathematical basis of encryption, affine encryption	Discussion, lecture, message exchange
evening	Matrices I	Read handout, do exercises	
DAY 7 Tuesday	morning	Modular Arithmetic II	Turn in exercises
		Create your own cryptosystem	Students work on presentations
	evening	Study for midterm	
DAY 8 Wednesday	morning	Matrices II	Handout
	afternoon	Matrix Encryption	Lecture, cipher crack
		Create your own cryptosystem	Student cipher presentations
evening	Study for midterm		
DAY 9 Thursday	morning	Midterm examination	
	afternoon	Introduction to machine ciphers, history of the Enigma	Discussion, Lecture
		Permutations I	Lecture, handout
evening	Introduction to the Enigma, encryption	Create Enigma simulators	
DAY 10 Friday	morning	Enigma encryption and decryption	Message exchange
	afternoon	Introduction to Enigma crack	Lecture
		Continued Enigma crack	Lecture
evening	Permutations II	Lecture, handout	
DAY 10 Friday	morning	Euler Phi function	Lecture, create function table, discussion
	afternoon	Still more Enigma crack	Cipher crack as class, in groups
	afternoon	Last of the Enigma	

WEEK THREE

Day	Time	What (knowledge goals/concepts/reading)	How (activities)
Sunday	evening	Binary arithmetic	Lecture, handout
		Xenocryptology	Analyze radio telescope message
DAY 11 Monday	morning	History of cryptology	Field trip to the National Cryptologic Museum
	afternoon	Field trip	Field trip
	evening	Introduction to digital cryptosystems, Linear Shift Registers	Lecture, handout
DAY 12 Tuesday	morning	Modular exponentiation	Lecture, handout
		Block ciphers, mini-DES	Lecture
	afternoon	Modular exponentiation	Work on exercises
		Issues with digital security	Discussion
evening	Diffie-Hellman Key Exchange and Mini-DES	Lecture key and message exchange in partners	
DAY 13 Wednesday	morning	Fermat's and Euler's Theorems	Lecture
		Public-key cryptography, RSA encryption	Discussion, lecture
	afternoon	RSA	Cipher crack in groups
		Digital authentication with RSA	Discussion
evening	Post-Assessment		
DAY 14 Thursday	morning	Final Exam	
	afternoon	Final Exam	
	evening	Final Exam	
DAY 15 Friday	morning	Course Wrap-up	SPEs