CTY Course Syllabus
Cryptology

Day	Time	What (Knowledge, concepts, reading)	How (activities)
WEEK ONE			
DAY 1 Monday	Morning	• Course Intro & Honor Code • Pre-Assessment • Icebreaker • Caesar Shift Cipher	• Discussion • As individuals • Decrypt Names and discuss strategy • Caesar wheel construction and practice problems
	Afternoon	• Combinatorics: counting principle, combinations, permutations • Monoalphabetic substitution ciphers with spaces	• Inquiry lesson & begin exercises 1-6 • Lesson, read The Code Book (TCB) pgs. 20-25 & practice encryption/decryption, key strength discussion
	Evening	• History of cryptology • Monoalphabetic substitution ciphers with spaces • Practice cracking Caesar shift ciphers	• Read TCB Intro, pgs. 1-14 • Finish classwork and complete examples, pgs. 20-21 • Decode cruel and unusual Caesar examples, extra challenge problems
DAY 2 Tuesday	Morning	• Warm up and finish combinatorics • Intro to Cryptology • Monoalphabetic substitution without spacing • Divisibility rules	• Combinatorics exercises 1-6 • Discussion on history and vocabulary • Conduct frequency analysis as a class • Brief topics review and work on problems individually
	Afternoon	• More monoalphabetic substitution	• More practice examples using student hints • For encoding, show example with keyboard and practice in pairs
	Evening	• History – Mary, Queen of Scots Plot	• Read TCB pgs. 14-44 & Appendices A and C

Day	Time	What (Knowledge, concepts, reading)	How (activities)
		• Additional monoalphabetic and combinatorics practice	• Finish working on cipher (without spaces) practice, do additional combinatorics exercises 1-6
DAY 3 Wednesday	Morning	• Intro to Vigenere cipher • Encryption/decryption • Cracking Vigenere by finding keyword length + frequency analysis • Practice encryption, decryption, analysis of Caesar, mono sub, Vigenere	• Presentation • Activity for pairs • Begin Vigenere example 1 • Computer lab activity
	Afternoon	• Continue Vigenere • Division and Euclidean algorithms	• Finish example 1 • Mini-lesson and exercises
	Evening	• Vigenere cipher • More vigenere practice	• Read TCB pgs. 45-78 • Decrypt Vigenere example 2 in pairs
DAY 4 Thursday	Morning	• Skills Practice • Vigenere summary • One-time pad intro • One-time pad practice • Extended Euclidean Algorithm (EEA)	• Group competition • Strengths/Weaknesses discussion • Mini-lesson • Revolutionary War example 1 – work in groups • Lesson and begin exercises
	Afternoon	• Practice with EEA • More cracking the one-time pad	• Exercises • Revolutionary War example 2
	Evening	• Mechanization of secrecy • Practice one-time pad decryption	• Read TCB pgs. 79-100; 115-124; Appendix G • Finish Revolutionary War one-time pad exercises
DAY 5 Friday	Morning	• Intro to Playfair cipher and cribbing • Practice cracking Playfair	• Practice encryption/decryption, cracking with a crib • Read TCB Appendix E and complete exercises
	Afternoon	• Intro to Modular Arithmetic • Practice modular arithmetic	• Mini-lesson • Exercises
	Evening	• More practice with EEA • First week review	• EEA Exercises • Group challenges in breaking 1st week ciphers

Day	Time	What (Knowledge, concepts, reading)	How (activities)
WEEK TWO			
DAY 6 Monday	Morning	• Multiplicative inverses in modular arithmetic • Intro to encryption/decryption with the Affine cipher	• Mini Lesson and individual/pair exercises • Mini Lesson and individual/group exercises
	Afternoon	• Practice encryption/decryption with the Affine cipher	• Practice Affine cipher exercises
	Evening	• More encryption/decryption with the Affine cipher • ADFGVX cipher and Zimmerman telegram	• Finish Affine cipher exercises • Mini TA lesson and read TCB pgs. 101-115 and Appendix F
DAY 7 Tuesday	Morning	• ADFGVX cipher • ADFGVX decryption • Cracking the ADFGVX cipher	• Encryption example as class • Decryption exercise • Cracking exercise
	Afternoon	• Matrix addition, multiplication, inverses • Modular matrices • Hill cipher intro	• Mini-lesson and matrices exercises 1-4 • Mini-lesson and modular matrices exercise 1-3 • Mini-lesson and Hill cipher exercises 1-6
	Evening	• Practice with Hill and ADFGVX ciphers • Review manual encryption	• Finish ADFGVX and Hill cracking exercises • Practice mid-term exam
DAY 8 Wednesday	Morning	• Midterm • Intro to Machine Ciphers and History of Enigma • Enigma demonstration	• Activity • Class discussion and mini-lesson • Short video: James Grime demonstration
	Afternoon	• Enigma encryption and decryption practice • Enigma keyspace calculations	• Computer lab activity • Challenge problem
	Evening	• Enigma history • Bletchley Park • Student designed cryptosystem	• Read TCB pgs. 124-142 • Short video • Brainstorming and practice with student invented cryptosystems; start writing letter home.

Day	Time	What (Knowledge, concepts, reading)	How (activities)
DAY 9 Thursday	Morning	• Permutations	• Mini-lesson and exercises
	Afternoon	• Cracking the Enigma	• Enigma simulator creating
	Evening	• Cracking the Enigma • Student designed cryptosystem	• Read TCB pgs. 143-189 • Finish letter and design poster presentation
DAY 10 Friday	Morning	• Presentation on cryptosystems • Practice cracking the Enigma	• Individual presentations • Enigma exercises 1, 2
	Afternoon	• Binary and hex numbers • Digital Encryption, Linear Feedback Shift Registers	• Inquiry lesson and exercises 1-5 • Mini-lesson and exercises 1-6
	Evening	• The Language Barrier • Midterm continued	• Read TCB pgs. 192-242, Appendix J • Additional work on midterm activity
WEEK THREE			
DAY 11 Monday	Morning	• Fast exponentiation • One-way functions and the discrete log problem • Diffie-Hellman Key Exchange • Practice Diffie-Hellman	• Group activity and exercises 1-4 • Mini-lesson • Demonstration (INST/TA) • Pair practice using small mod values
	Afternoon	• Applications and Symmetric-key algorithms	• Mini-lesson and history, class discussion
	Evening	• Midterm continued	• Final round for activity
DAY 12 Tuesday	Morning	• RSA introduction	• Demonstration (INST/TA), mini-lesson, discussion
	Afternoon	• Practice RSA • RSA analysis	• Send RSA messages (small mod values) to partners • RSA exercises 1-4
	Evening	• Public Key Encryption • What makes a good problem?	• Read TCB pgs. 243-292, Appendix J • Discussion
DAY 13 Wednesday	Morning	• Block ciphers, non-brute force attacks on modern systems • More discrete logarithm applications and cryptosystem bases	• Mini-lesson, demonstration (INST/TA) • Mini-lesson, group activity

Day	Time	What (Knowledge, concepts, reading)	How (activities)
	Afternoon	• Quantum Cryptography • Course review	• Mini-lesson, group activity, discussion • Review problems, discussion
	Evening	• Post-Assessment	
DAY 14 Thursday	Morning	• Final Exam Part I	
	Afternoon	• Final Exam Part II	
	Evening	• Privacy issues	• Discussion/debate
DAY 15 Friday	Morning	• Course wrap-up, crypto game • SPEs, goodbyes	