

# Cryptology

## CTY Course Syllabus

Day	Session	What	How
Day 1 Monday	Morning	<ul style="list-style-type: none"> <li>• Welcome and Introduction to course</li> <li>• Pre-assessment</li> <li>• Basics of Cryptology</li> <li>• Transposition</li> <li>• Caesar Shift</li> </ul>	<ul style="list-style-type: none"> <li>• Icebreaker, discuss class and CTY rules (brainstorm as a class)</li> <li>• Check Roster and sign contracts</li> <li>• Administer Pre-Assessment</li> <li>• Define basic cryptology terms</li> <li>• Rail fence and scytale</li> <li>• Make Caesar wheel and decode examples</li> </ul>
	Afternoon	<ul style="list-style-type: none"> <li>• Basis Monoalphabetic ciphers</li> <li>• Combinatorics – counting principle, combinations and probability</li> </ul>	<ul style="list-style-type: none"> <li>• Lesson and examples encoding/decoding Caesar Shift and Rail Fence ciphers</li> <li>• Discuss strength</li> </ul>
	Evening	<ul style="list-style-type: none"> <li>• History – Caesar Shift</li> <li>• Practice Combinatorics</li> </ul>	<ul style="list-style-type: none"> <li>• Read <i>The Code Book</i> (intro, 1-14) + write 2 questions about reading</li> <li>• More Combinatorics Wkst</li> <li>• Cruel Caesar Examples if needed</li> </ul>
Day 2 Tuesday	Morning	<ul style="list-style-type: none"> <li>• Warm-Up+Finish Combinatorics</li> <li>• Questions/comments @ <i>Code Book</i></li> <li>• Monoalphabetic Substitution Cipher with spacing and punctuation</li> <li>• Decoding Monoalphabetic Substitution Cipher without spacing</li> </ul>	<ul style="list-style-type: none"> <li>• Caesar Shift problem</li> <li>• Collect and go over as a class</li> <li>• Probability and Frequency Analysis</li> </ul>
	Afternoon	<ul style="list-style-type: none"> <li>• More decoding Monoalphabetic Ciphers practice</li> <li>• Encode Monoalphs</li> </ul>	<ul style="list-style-type: none"> <li>• Practice Examples – strong students give hints to those getting stuck</li> <li>• Show/encode ex with keyword and practice with partner</li> </ul>
	Evening	<ul style="list-style-type: none"> <li>• History – Queen Mary of Scots Plot</li> <li>• Practice Substitution Ciphers</li> </ul>	<ul style="list-style-type: none"> <li>• Read <i>The Code Book</i> (14-44) and pg. 375 (PigPen Cipher) (<i>Extra: Ch. 5 if done early</i>)</li> <li>• Practice Examples for monoalphs</li> </ul>
Day 3 Wednesday	Morning	<ul style="list-style-type: none"> <li>• Warm-up</li> <li>• Polyalphabetic Substitution Cipher</li> <li>• Vigenère Cipher</li> <li>• Division Algorithm + Euclidean Algorithm</li> </ul>	<ul style="list-style-type: none"> <li>• Read pg. 45-51</li> <li>• Swapping alphabets – use <a href="http://simonsingh.net">simonsingh.net</a></li> <li>• Encoding example using <a href="http://SimonSingh.net">SimonSingh.net</a> and book</li> <li>• Use notes and practice examples (hold onto work for EEA lesson)</li> </ul>

Day	Session	What	How
	Afternoon	<ul style="list-style-type: none"> <li>Decoding Vigenère Cipher</li> </ul>	<ul style="list-style-type: none"> <li>Babbage-Kasiski attack</li> </ul>
	Evening	<ul style="list-style-type: none"> <li>History of Vigenère + practice decoding</li> </ul>	<ul style="list-style-type: none"> <li>Read <i>The Code Book</i> (52-99, skim 70-77 since covered in class)</li> </ul>
Day 4 Thursday	Morning	<ul style="list-style-type: none"> <li>Thurs Morning Wake-Up!</li> <li>Practice Vigenère</li> <li>Index of Coincidence</li> </ul>	<ul style="list-style-type: none"> <li>Decode Caesar and Vigenère</li> <li>Continue examples from Wed. and answer lab questions</li> <li>Find key length using example</li> </ul>
	Afternoon	<ul style="list-style-type: none"> <li>Playfair</li> <li>Tell about Group challenge Friday</li> </ul>	<ul style="list-style-type: none"> <li>Go through in example in notes</li> <li>Practice with “Dear Chuck”</li> </ul>
	Evening	<ul style="list-style-type: none"> <li>Cryptography in literature</li> <li>Practice deciphering codes</li> </ul>	<ul style="list-style-type: none"> <li>Read <i>Dancing Men</i> by A.C. Doyle</li> <li>Finish monoalph, Vigenère codes in groups for Friday</li> </ul>
Day 5 Friday	Morning	<ul style="list-style-type: none"> <li>Quiz (review gcd first)</li> <li>Encode/Decode Playfair</li> </ul>	<ul style="list-style-type: none"> <li>Ciphers using keywords and history questions</li> <li>Use notes and examples</li> </ul>
	Afternoon	<ul style="list-style-type: none"> <li>Caesar Shift, monoalphs and Vigenère Cipher Competition</li> </ul>	<ul style="list-style-type: none"> <li>Compete in teams against other Code Class</li> </ul>
Sunday	Evening	<ul style="list-style-type: none"> <li>Math concepts practice</li> <li>Begin Design Cryptosystem Project</li> </ul>	<ul style="list-style-type: none"> <li>Practice Problems on Modular and Extended Euclid. Theorem</li> <li>See handout</li> </ul>
Day 6 Monday	Morning	<ul style="list-style-type: none"> <li>Crack Playfair</li> <li>ADFGVX cipher</li> </ul>	<ul style="list-style-type: none"> <li>Use class examples and cribbing</li> <li>How it works, encrypt/decrypt</li> </ul>
	Afternoon	<ul style="list-style-type: none"> <li>Work on cryptosystems</li> </ul>	<ul style="list-style-type: none"> <li>Check system with instructor and put on poster board</li> </ul>
	Evening	<ul style="list-style-type: none"> <li>Intro to Enigma</li> <li>Work on Cryptosystems</li> </ul>	<ul style="list-style-type: none"> <li>Read <i>The Code Book</i> pg. 101-142 and pg. 381 (one-time pad)</li> <li>Q&amp;A (see Word document)</li> </ul>
Day 7 Tuesday	Morning	<ul style="list-style-type: none"> <li>Finish ADFGVX cipher</li> <li>Modular arithmetic and inverses</li> </ul>	<ul style="list-style-type: none"> <li>Encode and decode in partners using keywords (see handout)</li> <li>Notes and examples</li> </ul>
	Afternoon	<ul style="list-style-type: none"> <li>Finish Cryptosystems</li> <li>Practice Playfair</li> </ul>	<ul style="list-style-type: none"> <li>Finish posters and make presentation schedule</li> <li>Use handout examples</li> </ul>

Day	Session	What	How
	Evening	<ul style="list-style-type: none"> <li>History of Enigma Machine</li> </ul>	<ul style="list-style-type: none"> <li>Nova Enigma Video “Decoding Nazi Secrets” (2 hrs)</li> </ul>
Day 8 Wednesday	Morning	<ul style="list-style-type: none"> <li>Questions/comments about video</li> <li>Practice Modular Arithmetic</li> <li>Affine Cipher</li> </ul>	<ul style="list-style-type: none"> <li>Class discussion</li> <li>Bingo</li> <li>Encoding and Decoding using inverses</li> </ul>
	Afternoon	<ul style="list-style-type: none"> <li>Cryptosystem Presentations</li> </ul>	<ul style="list-style-type: none"> <li>15 minutes each</li> </ul>
	Evening	<ul style="list-style-type: none"> <li>Cracking the Enigma</li> <li>Study for Quiz</li> </ul>	<ul style="list-style-type: none"> <li>Read <i>The Code Book</i> pg. 143-189 <ul style="list-style-type: none"> <li>Write 2 questions/comments</li> </ul> </li> <li>Practice gcd, EEA, mod arith., and matrices</li> </ul>
Day 9 Thursday	Morning	<ul style="list-style-type: none"> <li>Encoding and Decoding Hill’s System (Matrices)</li> <li>Cryptosystem Presentations</li> </ul>	<ul style="list-style-type: none"> <li>Use class notes and calculator</li> <li>15 minutes each</li> </ul>
	Afternoon	<ul style="list-style-type: none"> <li>Encoding and Decoding Hill’s System (Matrices)</li> </ul>	<ul style="list-style-type: none"> <li>Use class notes</li> </ul>
	Evening	<ul style="list-style-type: none"> <li>Encode/Decode matrix problems (Hill’s System)</li> <li>Practice Modular, gcd, EEA and matrices</li> </ul>	<ul style="list-style-type: none"> <li>Students work in groups using same key but individual plaintext</li> <li>Use handout</li> </ul>
Day 10 Friday	Morning	<ul style="list-style-type: none"> <li>Finish practice worksheet</li> <li>Cracking Hill’s System</li> <li>Paper Enigma Machines</li> </ul>	<ul style="list-style-type: none"> <li>Use handout from Evening</li> <li>Go through notes and examples</li> <li>Make simulators</li> </ul>
	Afternoon	<ul style="list-style-type: none"> <li>Quiz 2 (about 1 hr)</li> </ul>	<ul style="list-style-type: none"> <li>Modular, gcd, EEA and matrices</li> </ul>
Sunday	Evening	<ul style="list-style-type: none"> <li>Public Key Cryptography</li> <li>Hand back quizzes</li> <li>Practice Hill’s System and finding inverses</li> </ul>	<ul style="list-style-type: none"> <li>Read <i>The Code Book</i> pg. 243-292 (Can work on Code B ciphers)</li> <li>White Board Review in pairs</li> </ul>
Day 11 Monday	Morning	<ul style="list-style-type: none"> <li>Answer questions about Enigma</li> <li>Warm-Up Enigma ex.</li> <li>Permutations/Cycle Structure</li> </ul>	<ul style="list-style-type: none"> <li>Use written questions to earlier reading</li> <li>Decode Class ex. #1 using simulator</li> <li>Go through notes with examples</li> </ul>
	Afternoon	<ul style="list-style-type: none"> <li>Rejewski’s crack of the Enigma</li> </ul>	<ul style="list-style-type: none"> <li>Go through notes with example and simulator</li> </ul>

Day	Session	What	How
	Evening	<ul style="list-style-type: none"> <li>• Pretty Good Privacy</li> <li>• Finish codes for CODE B class</li> </ul>	<ul style="list-style-type: none"> <li>• Read <i>The Code Book</i> pg. 293-316</li> <li>• Write opinion on strong encryption vs. government restrictions</li> </ul>
Day 12 Tuesday	Morning	<ul style="list-style-type: none"> <li>• Enigma Crack</li> <li>• Binary and Hexadecimal systems</li> </ul>	<ul style="list-style-type: none"> <li>• Use class notes and examples with simulator</li> </ul>
	Afternoon	<ul style="list-style-type: none"> <li>• Application of Binary encoding</li> </ul>	<ul style="list-style-type: none"> <li>• Examples of binary to express pictures and sound</li> </ul>
	Evening	<ul style="list-style-type: none"> <li>• Future Cryptography</li> <li>• Practice Binary + Hexadecimal</li> <li>• Fast Exponentiation</li> </ul>	<ul style="list-style-type: none"> <li>• Read <i>The Code Book</i> pg. 317-350</li> <li>• Use worksheet with examples</li> </ul>
Day 13 Wednesday	Morning	<ul style="list-style-type: none"> <li>• Practice Fast Exponentiation</li> <li>• RSA</li> </ul>	<ul style="list-style-type: none"> <li>• Use notes and examples</li> <li>• Use notes and go through Alice + Bob example</li> </ul>
	Afternoon	<ul style="list-style-type: none"> <li>• Watch <i>Sneakers</i> (2 hrs)</li> </ul>	
	Evening	<ul style="list-style-type: none"> <li>• Study for Final Exam</li> <li>• Binary, Hexadecimal, gcd, inverse review</li> </ul>	<ul style="list-style-type: none"> <li>• Brainstorm list of main ciphers covered in class and key features of each and present</li> <li>• White board review in pairs</li> </ul>
Day 14 Thursday	Morning	<ul style="list-style-type: none"> <li>• Course Evaluations</li> <li>• Final Exam Part I + II</li> </ul>	<ul style="list-style-type: none"> <li>• Student Program Evaluations (SPEs)</li> <li>• Post-Assessment</li> </ul>
	Afternoon	<ul style="list-style-type: none"> <li>• Final Exam Part II</li> </ul>	<ul style="list-style-type: none"> <li>• Post-Assessment</li> </ul>
Day 15 Friday	Morning	<ul style="list-style-type: none"> <li>• Evaluations, Goodbyes, Game Theory Casino</li> </ul>	<ul style="list-style-type: none"> <li>• Give out Certificates</li> </ul>