University of Wisconsin-Madison
Department of Electrical and Computer Engineering
CS/ECE/Math 435 - Introduction to Cryptography, Spring Semester 2021
Course Information and Administration

Instructor:	Professor Christopher L. DeMarco, Electrical and Computer Engineering Office Hours – Tuesdays 10:00 AM - 11:30 AM; Thursdays 11:30 AM – 1:00 PM e-mail: cdemarco@wisc.edu Campus Office: Rm. 3417 Engineering Hall; phone: (608) 262-5546
TA:	Tommy Yee, tyee2@wisc.edu Office Hours – Mondays & Fridays 2:00 PM- 3:30 PM (beginning 29 Jan)
Course Web Resources:	via Canvas course webpage; on-line lectures and virtual office hours via Blackboard Collaborate ("BBCollaborate Ultra" tab on the 435 Canvas page)
Weekly Assessment:	Assignments will be distributed via Canvas on Fridays, to be completed by the following Friday (one week). HW assignments involve computations, evaluation of algorithms, and/or proofs. However, full student work will not be submitted. Instead, associated with each assignment will be a weekly Canvas quiz, with questions closely tied to work required in the HW assignment. ***Quiz completion deadline will be 4:00 PM Fridays***. Instructional HW assignment solutions will be posted in Canvas the following week.
Exams:	One evening exam and a final. The midterm exam is tentatively scheduled for Thursday, March 18, 7:15-9:15 PM. Final Exam – Sunday, May 2, 10:05 AM - 12:05 PM. These exams will be administered on-line, employing UW-Madison's implementation of "Honorlock," the automated proctoring service.
Grading Weights:	Assignment-based quizzes: 18%, Midterm Exam 34%, Final 48%. Lowest quiz grade dropped.
Software:	Many of algorithms of interest in this course involve algebraic operations on finite fields; a package for computer-assisted algebra is a valuable tool. Demonstrations in lecture, and HW assignment solutions will use MATLAB: (www.mathworks.com/academia/tah-portal/university-of-wisconsin-madison-678095.html). Other languages and packages can provide comparable functionality. Students are free to use other environments if they wish, but MATLAB will be the default, recommended computational environment for 435.

Required Text: The primary text for the course will be "*Course Notes for Introduction to Cryptography*," copyright 2019, written by UW-Madison Computer Sciences faculty member Professor Eric Bach. These notes were created specifically for CS/ECE/Math 435, and are organized by lecture. The lecture schedule for this semester will follow this structure, with minor accommodation for the non-standard schedule of the Spring 2021 semester.

Professor Bach has generously agreed to make this text available at no cost to 435 students - it is available in a watermarked pdf format under the "Files" tab of the CS/ECE/Math 435 Canvas page. ***PLEASE RECIPROCATE PROF. BACH'S CONSIDERATION BY RESPECTING HIS COPYRIGHT***. This pdf copy is intended solely for the personal educational use of UW-Madison students enrolled CS/ECE/Math 435 for the Spring 2021 semester; further electronic distribution is strictly prohibited. Transfer of a single hardcopy is permissible, as typical with a textbook.

Optional Text: J. Katz, and Y. Lindell, "*Introduction to Modern Cryptography*." This text was released in its third edition in December 2020; as of early January 2021, this edition's availability is very limited at textbook retailers. The updates are not critical to coverage in CS/ECE/Math 435; the 2014 second edition is therefore adequate. Students may find purchase of this text useful, but it is optional. **NOTE**: The 2014 2nd edition is available through the UW Libraries via ProQuest Ebook Central. Ebook Central limits the number of simultaneous electronic checkouts of this book. Please do NOT electronically check it out. Instead please use the "Read Online" tab, to facilitate wider access by students.

Topics (Organized by lecture number, consistent with E. Bach's course notes):

1. Introduction
2. Modular Arithmetic, Affine Ciphers
3. Euclidean Algorithm, Inverse mod N
4. Monoalphabetic and Polyalphabetic Ciphers
5. Hill Ciphers, Matrices mod N
6. Transposition Ciphers
7. Intro to Cryptanalysis; Probability Models
8. Key Enumeration; Known/Chosen Plaintext Attacks
9. Correlation Attacks on Shift Ciphers

10. Letter Frequencies, Probable Words
11. Monoalphabetic Cryptanalysis, Kasiski's Test
12. Coincidence Index
13. Polyalphabetic Cryptanalysis
14. Entropy
15. Key Equivocation
16. Perfect Secrecy
17. Stream Ciphers and the One-time Pad
18. Keystreams from Iterated Affine Maps
19. Keystreams from Decimal Expansions
20. Linear Shift Register Sequences
21. LFSR Cryptanalysis using Linear Algebra
22. Berlekamp-Massey Algorithm
23. Nonlinear Feedback Shift Registers
24. Stream Ciphers Incorporating Nonlinearity
25. Block Ciphers and Operation Modes
26. Feistel Ciphers
27. DES: The Gory Details
28. Birthday Attacks on Multiple Encryption
29. Finite Fields
30. The Advanced Encryption Standard (AES)
31. More Block Ciphers: IDEA and Skipjack
32. Big Number Arithmetic
33. Faster Multiplication and Division
34. Exponentiation
35. The RSA System
36. Key Generation, Primality and Factoring
37. Discrete Logarithms, Diffie-Hellman Key Exchange
38. More on Diffie-Hellman, KEA
39. Password Encryption
40. Authentication in Networks, Kerberos
41. Digital Signatures via RSA
42. The ElGamal digital signature scheme
43. Cryptographic hash functions