MAKING BREAKING CODES (FALL 2021)
SYLLABUS AND HOMEWORK

Textbook: *Introduction to Cryptography with Coding Theory (2nd Edition)*
by Wade Trappe and Lawrence Washington

Sept 9 - Sept 17: EARLY CRYPTOGRAPHY, VIGENÈRE CIPHER,
EUCLIDEAN ALGORITHM
(pp. 12 - 24, 63 - 75 in the textbook)

Week of Sept 20: FERMAT-EULER THEOREM, RSA CRYPTOSYSTEM
(pp. 79 - 82, 85 - 86, 164 - 169 in the textbook)

Week of Sept 27: DISCRETE LOG'S
DIFFIE HELLMAN CRYPTOSYSTEM
(pp. 201 - 206, 211 - 214 in the textbook)

EXAM 1: Thursday, October 7

Week of Oct 11: CHINESE REMAINDER THEOREM
ATTACKS ON RSA & DIFFIE HELLMAN
MAN IN-THE-MIDDLE ATTACK
(pp. 76 -78, 182 -183, 203 -206, 257 -258 in the textbook)

Week of Oct 18: HASH FUNCTIONS
BIRTHDAY ATTACK
DIGITAL SIGNATURES
(pp. 218 - 223, 229 - 230, 244 - 252 in the textbook)

Week of Oct 25: ELLIPTIC CURVE CRYPTOGRAPHY
(pp. 347 -354 in the textbook)

Nov 4 - Nov 11: COIN FLIPPING
ZERO KNOWLEDGE PROOFS
(pp. 307 - 309, 316 - 321 in the textbook)

EXAM 2: Tuesday, November 16

Nov 18 - Nov 23: PRIME POLYNOMIALS
FINITE FIELDS
(pp. 93 -100 in the textbook)

Week of Nov 29: ERROR CORRECTING CODES
(pp. 392 -401 in the textbook)

Week of Dec 6: BINARY LINEAR CODES, SYNDROME DECODING
(pp. 408 - 415 in the textbook)