Content)

THEME: Alice wants to send Bob a message. Eve can easedrop. Hence Alice sends her message in code that Bob can decode. How can they do this so Eve cannot crack the code? How can Alice prove that she is Alice? We study these and related issues in a rigorous framework.

The list below is approximate in many ways. Some topics may end up not being covered Some may be for more or less lectures than indicated.

1. Classical Cryptography: Shift, Affine, Vigenere, Matrix, 1-time pads, breaking random generators, (4 lectures)
2. Public Key Cryptography based on Number Theory: Diffie Helman, ElGamal, RSA. (4 lectures)
3. Number Theory Algorithms to break Public Key. (3 lectures)
4. (2 lectures) Public Key Cryptography NOT based no Number Theory (called *post-quantum*). Learning with Errors
5. (3 lectures) Secret Sharing
6. (3 lectures) Digital Signatures and Authentication
7. (2 lectures) Cryptographic Hash Functions and their applications
8. (2 lectures) Psuedo Random Generators
9. (1 lecture) Guest lecture on censorship. (Not scheduled yet.)
10. (1 lecture) Guest lecture on the NIST post-quantum challenge. (Not scheduled yet.)

Possible other topics

1. The Quadratic Sieve Factoring Algorithm.
2. Message Authentication Codes (MAC).
3. Feistel Networks, MD5, AES, DES and other Real Systems

TEXT There is no text. There will be notes on line and slides on line.

PREREQUISITES (CMSC 106 OR CMSC 131 OR ENEE 150 OR Equiv Prog Exp) AND ((2 from CMSC 330, CMSC 351, ENEE 324, ENEE 380) OR (any of those and a 400-level MATH course) OR (two 400 level MATH courses) OR Permission of instructor.