Syllabus (Content)

Official name of the course:

CMSC/MATH/ENEE 456: Cryptology

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, (5 lectures)
2. Public Key Cryptography based on Number Theory: Diffie Helman, ElGamal, RSA. (4 lectures)
3. Number Theory Algorithms to break Public Key. (4 lectures)
4. (3 lectures) Public Key Cryptography NOT based no Number Theory (called *post-quantum*). Learning with Errors, McEliece.
5. (4 lectures) Secret Sharing
6. (3 lectures) What people really use: Stream Ciphers, Block Ciphes, Feistel Networks
7. (2 lectures) Cryptographic Hash Functions and their applications
8. (3 lectures) Digital Signatures and Authentication
9. (2 lectures) (if time) Block Chain and Bitcoin.