Syllabus (Content)

Official name of the course:

**CMSC/MATH/ENEE 456: Cryptology**

**THEME:** Alice wants to send Bob a message. Eve can eavesdrop. 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.

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 on 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. (time permitting) The Quadratic Sieve Factoring Algorithm.