Syllabus (Content)

Official name of the course:

CMSC/MATH 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 (Pre 1976) Cryptography: Shift, Affine, Vigenere, Matrix, 1-time pads. (3 lectures)
2. Public Key Cryptography: Diffie Helman, ElGamal, RSA. (3 lectures)
3. Number Theory Algorithms to break Public Key. (3 lectures)
4. Perfect Security and Perfect Randomness. (2 lectures)
5. Computational Security and Psuedorandm Genrators (2 lectures)
6. What people really use: Stream Ciphers. (2 lecture2)
7. What people really use: Block Ciphers. (2 lecture2)
8. Message Authentication Codes (MAC). (2 lectures)
9. Cryptographic Hash Functions and their applications (2 lectures)
10. Feistel Networks, MD5, AES, DES and other Real Systems (3 lectures)
11. Real RSA (1 lecture)
12. Digital Signatures (2 lectures)
13. Secret Sharing (2 lectures)