**Content of CMSC 389T: Advanced Discrete Strutures**
**Nickname: Discrete Math Plus Plus**

# 1 Topics to be covered

1. *Pre-modern Crypto:* How to exchange secret messages. Shift, Affine, Vig, Variants of Vig, Matrix, 1-time pad. And how to crack them.

2. *Modern Crypto:* Diffie Helman. Giant Step/Baby Step algorithm for Discrete Log. Other Discree Log Algorithm.

3. *Cracking Modern Crypto:* Quadratic Sieve Algorithm for factoring.

4. *Information Theoretic Security:* Secret Sharing with Cards. Secret Sharing with polynomials.

5. *Sharing Information without leaking it*

6. *Review of Combinatorics*: Permuatations, Combinations, Probabalistic Method.

7. *Misc* Generating functions, change-making problem,