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 key exchange. Discrete Log algorithms that may help to crack it.
3. *Modern Crypto:* RSA Public Key Crypto. Factoring algorithms that may help to crack it.
4. *Secret Sharing:* Secret Sharing with Cards. Secret Sharing with polynomials. Verifiable Secret Sharing.
5. *Cracking Passwords:* Hellman Tables and Rainbow Tables.
6. *Sharing Information without leaking it*