Content of CMSC 389T: Intro to cryptography

1 Overview

Here is the entire history of Cryptography:

1. Alice and Bob come up with a way to exchange secret messages so even if Eve intercepts them she decode them.
2. Alice and Bob prove that Eve cannot decode.
3. Eve decodes their messages.
4. Lather, rinse, repeat

We will present topics in cryptography with this point of view in mind. That is, we will present a code, show why it is uncrackable, and then crack it.

2 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.
3. *Modern Crypto:* RSA Public Key Crypto.
4. *Secret Sharing:* Secret Sharing with polynomials. Verifiable Secret Sharing.
5. *Optional topics depending on time and taste:* Algorithms for Discrete Log, Algorithms for Factoring, Secret Sharing with Cards (will need to review combinatorics), Error-detecting codes, Error-correcting codes, Cracking Passwords with Hellman Tables and Rainbow Tables, Sharing Information without leaking it, Muffinry.