Lecture 11: E-Mail Security

Date: October 21, 2013 ***Homework Due***: Nov. 1 at 5:00pm

1. Web identity
    a. Cryptographic Key Infrastructure
    b. Certificates (X.509, PGP)
    c. State and cookies
2. E-mail
    a. Structure of a letter: header fields, body, attachments
    b. How mail moves through the Internet: UAs, MTAs
    c. Mail addresses: MX records
3. E-mail and encryption
    a. Basic idea
    b. Interchange keys
    c. Data encryption key
    d. Doing the encryption
    e. Building the letter
    f. Decrypting the letter and verifying the signature
4. Mail relays
    a. Cypherpunk type 1 remailers
    b. Cypherpunk type 2 (mixmaster) remailers