Make Your Mark!

Digitally sign your e-mails.

Charlie Scott
cscott@infosec.utexas.edu
In days of yore...

- Imprinted wax seals were used on envelopes.
- The imprint was like a signature and proved who sent the letter.
- The unbroken wax seal proved the letter hadn’t been tampered with since imprinted.
Digital Signature: A Wax Seal for Today

- Applies a mathematical algorithm to an e-mail to create a short, unique representation of it (the wax).

- Uses a private cryptographic key to sign that representation (the imprint). This must be protected!

- The corresponding public key is signed by a trusted third party called a certificate authority (CA), proving that it belongs to the owner of the public/private key pair. Think of this as a notarized signature card.
To sign your e-mails...

- In MS Outlook:
  - Go to Tools → Trust Center → E-mail Security
  - Check “Add digital signature to outgoing messages”

- In Apple Mail
  - Create a New Message
  - Click on the checkmark in the lower right corner of the header pane.
When receiving an e-mail...

- Look for the seal on e-mails you get from coworkers.

  MS Outlook:  
  Apple Mail: 

- Verify the certificate is issued by our Certificate Authority (CA):

  MS Outlook:  
  Click on the seal ➔ Details ➔ signer’s e-mail address.

  Apple Mail:  
  Double click on the seal.