PGP Keysigning

- Don’t trust (anything), DO verify (everything)
- Components of a key
  - Fingerprint
    - UID collisions are possible, especially in RSA
    - Copyist errors (accidental or deliberate)
  - User ID
    - Usually a name and e-mail address
    - Verify the name by “authoritative” ID
    - Verify the e-mail address by sending the person mail
  - Key capabilities
    - Signing
    - Encryption

PGP Keysigning

- Suggested verification procedure
  - At the key signing event
    - Verify fingerprints
    - Verify ID
  - At home
    - Create a unique challenge for each UID
      - Encrypt (and sign) the challenge message for encryption keys
      - Sign the message for signing only keys
      - Maintain a record of the matches between challenge and UID
    - Send the challenge message(s) to each e-mail address, and request that the user return the challenge message to you, signed with their key (encryption optional)

PGP Keysigning

- Suggested verification procedure
  - Once the control of the private key is verified, sign each UID that has been verified, and send the signed key back to the person via the same e-mail address.
    - Trust: How much you trust the *person* to sign keys
    - Cert level: How well *you* have certified their identity
  - No need to send each signed UID separately, since you already verified that they can receive mail there
- Please try to do this “promptly,” as a matter of courtesy
- Key exchange service
  - https://biglumber.com/x/web?exchange=1