GNU Privacy Guard
Kevin Peng
Problem 1

- Alice wants to send a message to Bob
- Eve is eavesdropping
- How to securely communicate?
Solution 1: Symmetric-key cryptography

- Alice and Bob meet up and exchange a secret password
- Use password to encrypt everything
- Problem: need to physically meet
Solution 2: Public-Key Cryptography

- "Trapdoor functions" allow public-key cryptography
- Bob generates an public key and an associated private key
- Bob publishes public key, keeps private key secret
- Public key = lock, private key = key
- How Alice sends message to Bob:
  - Alice encrypts message with Bob’s public key
  - Alice sends encrypted message to Bob
- Bob decrypts with his private key
Problem 2

- Carol sends a message to Victor
- Victor wants to know if it’s legitimate
Solution

• Carol signs the message with private key
  – Kind of like inverse of encryption

• Victor uses public key to verify the signature
What is GPG

- Software program for securing communications
  - Ensuring confidentiality of messages by encryption
  - Ensuring authenticity of messages by signing
Demo of Sending a Message with GPG
Key Exchange

- How to obtain other’s public keys
- One method: physical exchange
Key Exchange

- Another method: keyservers
- Need to verify identity from keyservers!
  - Anyone can generate a fake keypair
Web of Trust

• I can trust keys that other responsible GPG users have verified
• To indicate trust in a key in GPG, sign it
• Example: Matt signs Chris’s key. I sign Matt’s key. If I download Chris’s key and it has Matt’s signature on it, I can trust Chris’s key
Levels of Trust

- **4 types by default:**
  - Unknown: I don’t know how responsible this user is
  - None: This user doesn’t verify keys properly at all
  - Marginal: This user kinda understands how to responsibly validate keys
  - Full: This user fully understands how to validate keys

- **Keys trusted if:**
  - One of the following conditions satisfied:
    - You signed it personally
    - Someone you fully trust signed it
    - Three marginally trusted people signed it
  - The chain of signatures is of length $\leq 5$
Group Demo