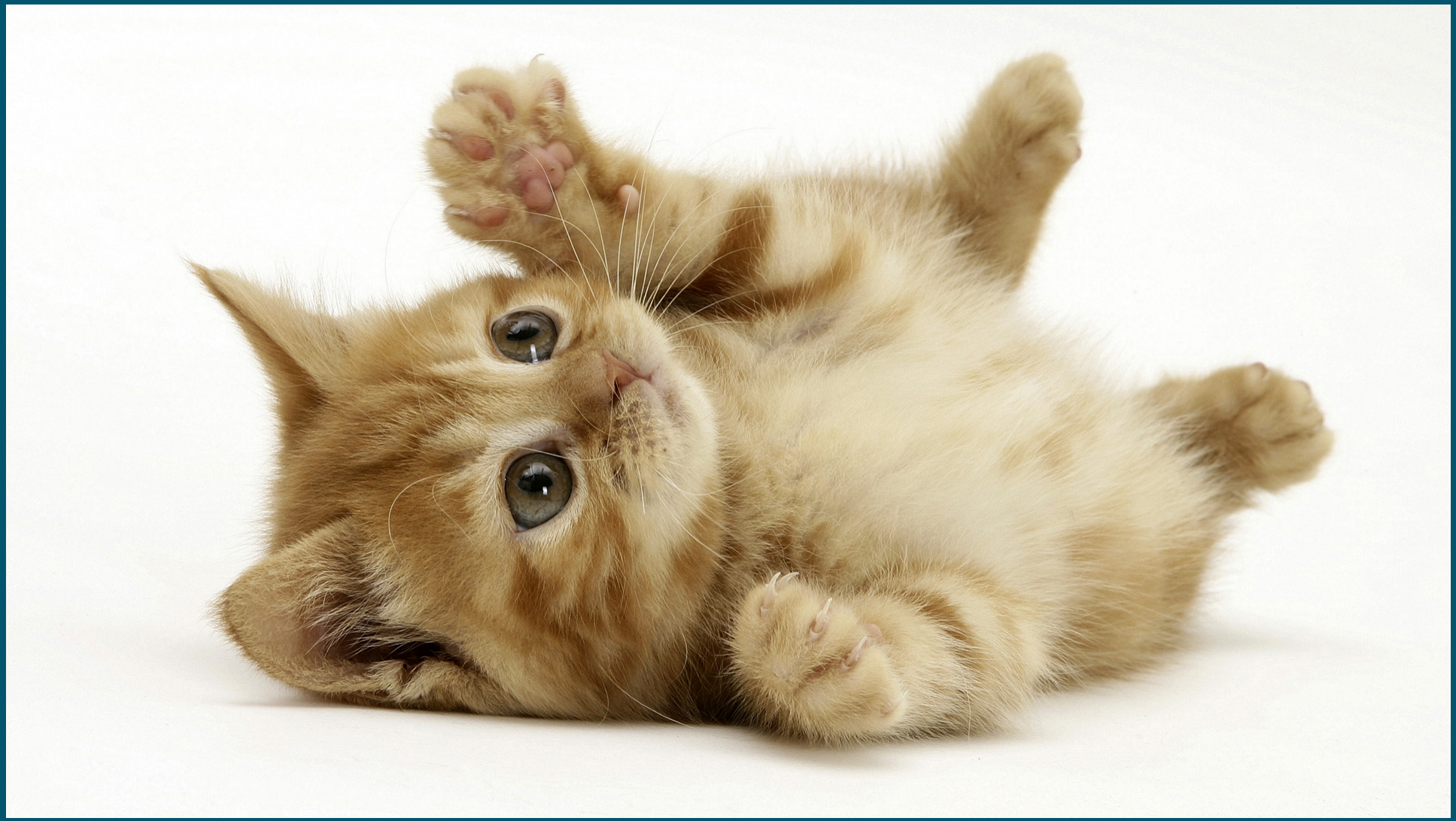
PGP KEYSIGNING PARTY

Hosted by

UCLA Linux Users Group

MOTIVATION



MOTIVATION

Let's be practical.

- Encrypt sensitive communication
  - Passwords, CC#, embarassing photos
  - Both ***you*** and your ***recipient's*** mailbox stores it
- Sign your messages
  - Prove that this message is sent by you

It's really easy to spoof email.

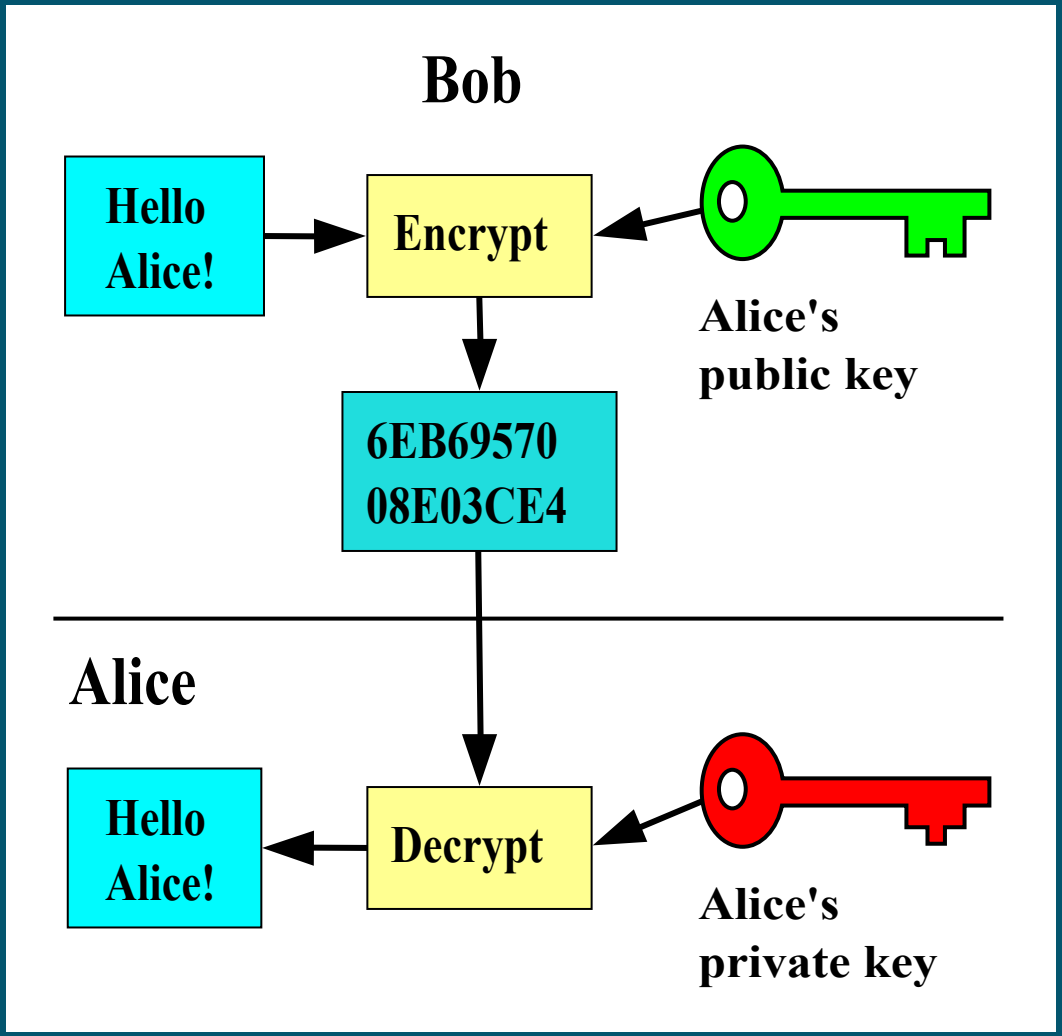
How to deal?

Asymmetric encryption

ASYMMETRIC ENCRYPTION

1. Each person has a *public* and a *private* key
2. People encrypt data to you using your *public* key
3. Only you can decrypt that data with your *private* key
4. ???
5. **Profit**

ASYMMETRIC ENCRYPTION



WHAT'S A KEY?

- Just a bunch of bytes (or a huge number)
- Asymmetric encryption simply means doing a lot of crazy math to transform between *plaintext* and *ciphertext*
- Private-encrypted can be public-decrypted, and vice versa
  - Signatures are private->public
  - Encryption is public->private

SO WHAT'S PGP?

PRETTY GOOD PRIVACY

- *Relies on* asymmetric encryption
- A public key distribution infrastructure
- Also a protocol for signing/encrypting emails

PGP? GPG? WTF?

- **GPG** is a ***tool*** that implements **PGP** the ***standard***
- Like a web browser vs the world wide web
- This means you interact with GPG most of the time
  - Useful generally for encrypting things, not just email

KEY DISTRIBUTION

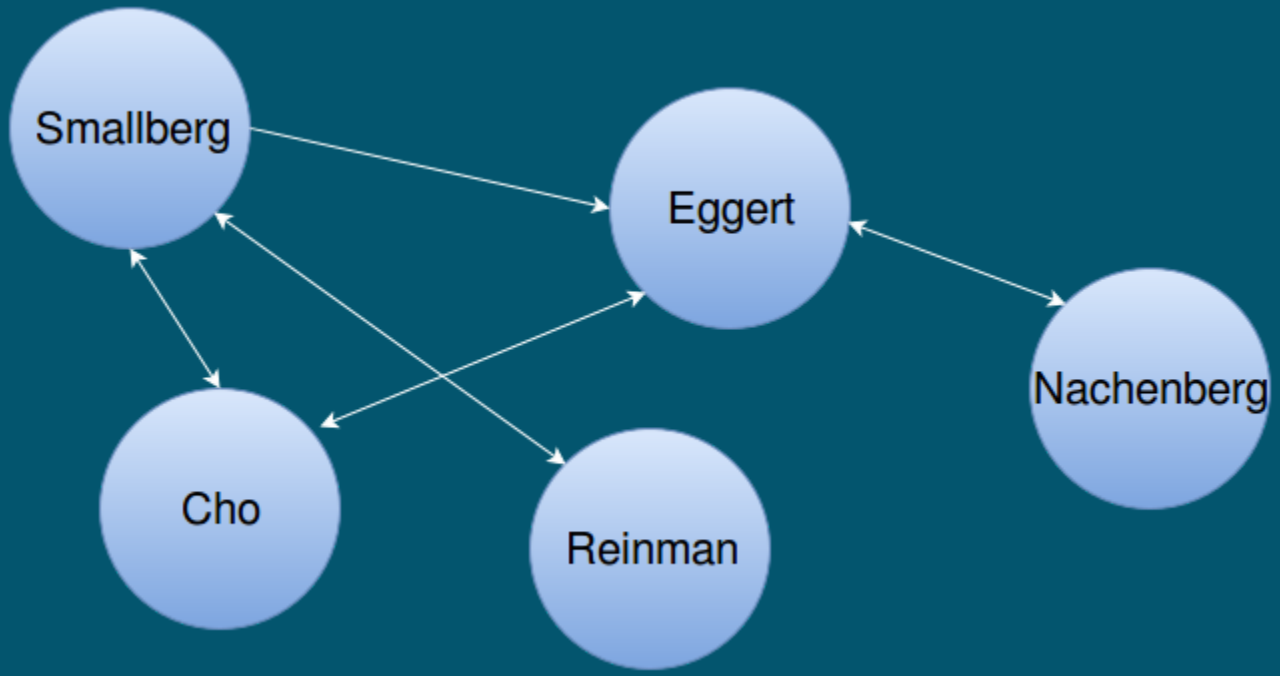
- You upload public key + identity to a *keyserver*
- Other people download key by searching for your name or email

WEB OF TRUST

- How do you verify a keyholder is really who they say they are?
  - Manually verify key fingerprint with each other
- You can *sign* somebody's key to leave a permanent proof of that

WEB OF TRUST

The graph of signatures and keys is the *web of trust*



USEFUL RESOURCES

- GPG Cheatsheet: http://irtfweb.ifa.hawaii.edu/~lockhart/gpg/gpg-cs.html
- GPG FAQ: https://www.gnupg.org/faq/gnupg-faq.html
- PGP key stats: http://pgp.cs.uu.nl/mk_path.cgi
- PGP global key stats: https://sks-keyservers.net/status/key_development.php
- (Windows) Gpg4win: https://www.gpg4win.org/index.html
- (Macs) GPGTools: https://gpgtools.tenderapp.com/kb/how-to/first-steps-where-do-i-start-where-do-i-begin-setup-gpgtools-create-a-new-key-your-first-encrypted-mail

KEYSIGNING PARTY

1. Receive a keylist from the host
2. Iterate over keylist together
   - Participant verifies their fingerprint is correct
     - first check
   - Host checks identity
     - second check

AFTER PARTY

```
# Import the key of everyone with two check marks
gpg --recv-keys <key ID 1> <key ID 2> ... <key ID N>

# Sign their keys
gpg --sign-key <key ID 1>
gpg --sign-key <key ID 2>
...
gpg --sign-key <key ID N>

# Send signatures to keyserver
gpg --send-keys <key ID 1> <key ID 2> ... <key ID N>
```

THANKS FOR COMING!