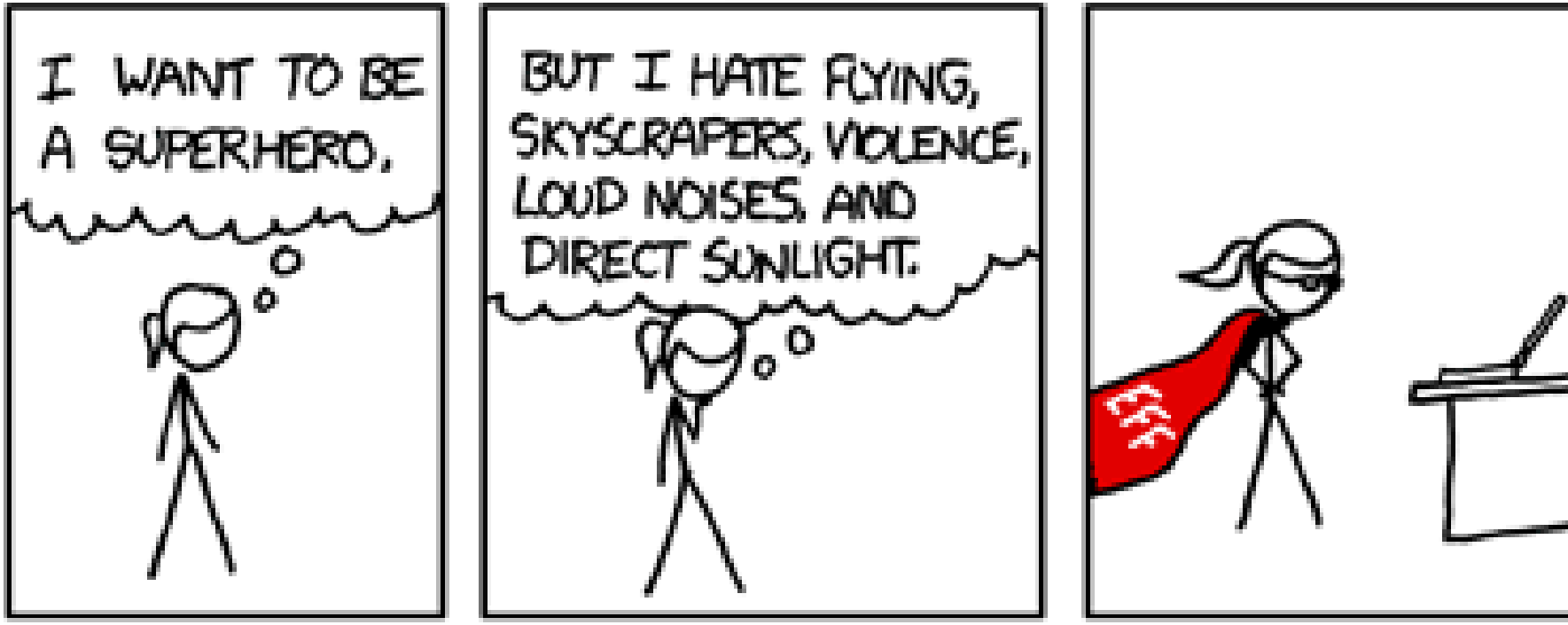
Concepts in Crypto

Parker Higgins parker@eff.org @xor
PGP: 4FF3 AA1B D29E 1638 32DE C765 9433 5F88 9A36 7709

Micah Lee micah@eff.org @micahflee
PGP: 5C17 6163 61BD 9F92 422A C08B B4D2 5A1E 9999 9697

Who We Are


I WANT TO BE A SUPERHERO.
BUT I HATE FLYING, SKYSCRAPERS, VIOLENCE, LOUD NOISES, AND DIRECT SUNLIGHT.
EFF

Fighting for Crypto Rights

ELECTRONIC FRONTIER FOUNDATION **https://www.eff.org**

Crypto Terminology

- Plaintext
- Key
- Ciphertext
- Public Key Crypto
- Symmetric Crypto

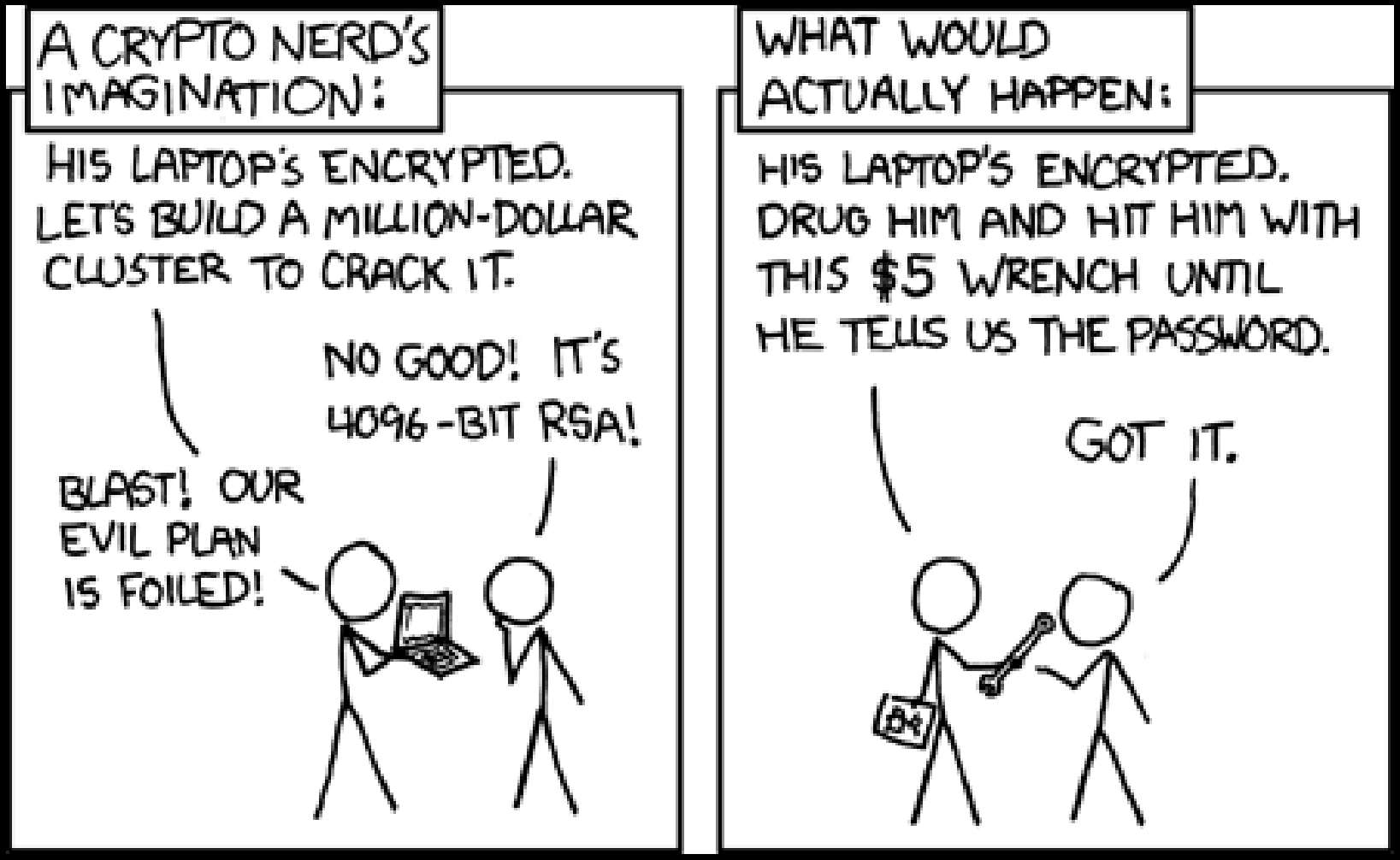
Open Source Crypto

- How your crypto works should not be a secret
- The **only** secret should be the key

- Through these covert partnerships [with tech companies], the agencies [like NSA] have inserted secret vulnerabilities known as backdoors or trapdoors into commercial encryption software.

  – The Guardian

Threat Modeling



Types of Encryption

- Transport encryption
  - HTTPS, when connecting to websites
- End to end encryption
  - PGP, Off-the-Record
- Disk encryption
  - TrueCrypt
  - FileVault
  - LUKS

Diffie-Hellman Key Exchange

How is it possible for two people to come up with a shared crypto key when everything is being spied on?

PGP: Pretty Good Privacy

- Originally written by Phil Zimmermann in 1991 for anti-nuclear weapons activists
- Keys are split into two halves:
  - Public key (share it widely)
  - Secret key (keep it secret, keep it safe)
- With a public key you can:
  - Encrypt messages that can only be decrypted with the associated secret key
  - Verify signatures that that were signed with the associated secret key
- With a secret key you can:
  - Decrypt messages that were encrypted with the associated public key
  - Digitally sign messages

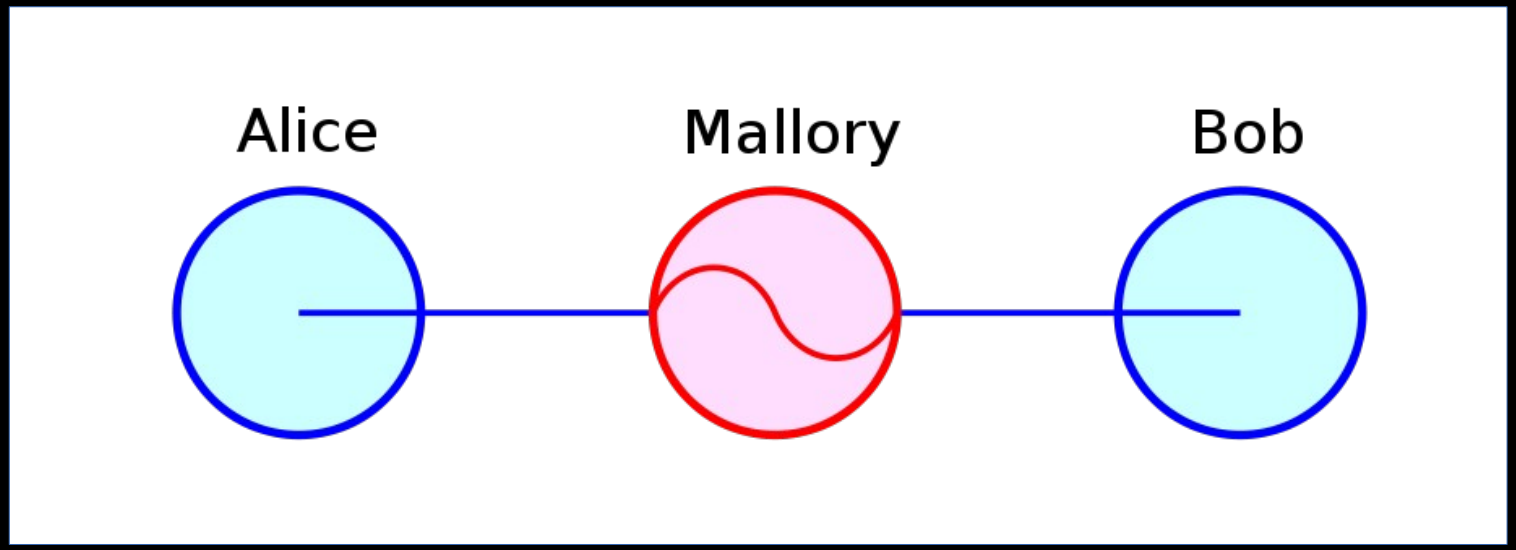
PGP in Practice

- GnuPG: open source implementation of OpenPGP (you shouldn't use the proprietary program called PGP)
- Thunderbird: a desktop email client, you can use it to check your email
- Enigmail: Thunderbird addon that adds OpenPGP functionality

HTTPS

- You already use it every day!
- End-to-end encryption between your **browser** and the website's **server**
- Install HTTPS Everywhere!
  https://www.eff.org/https-everywhere

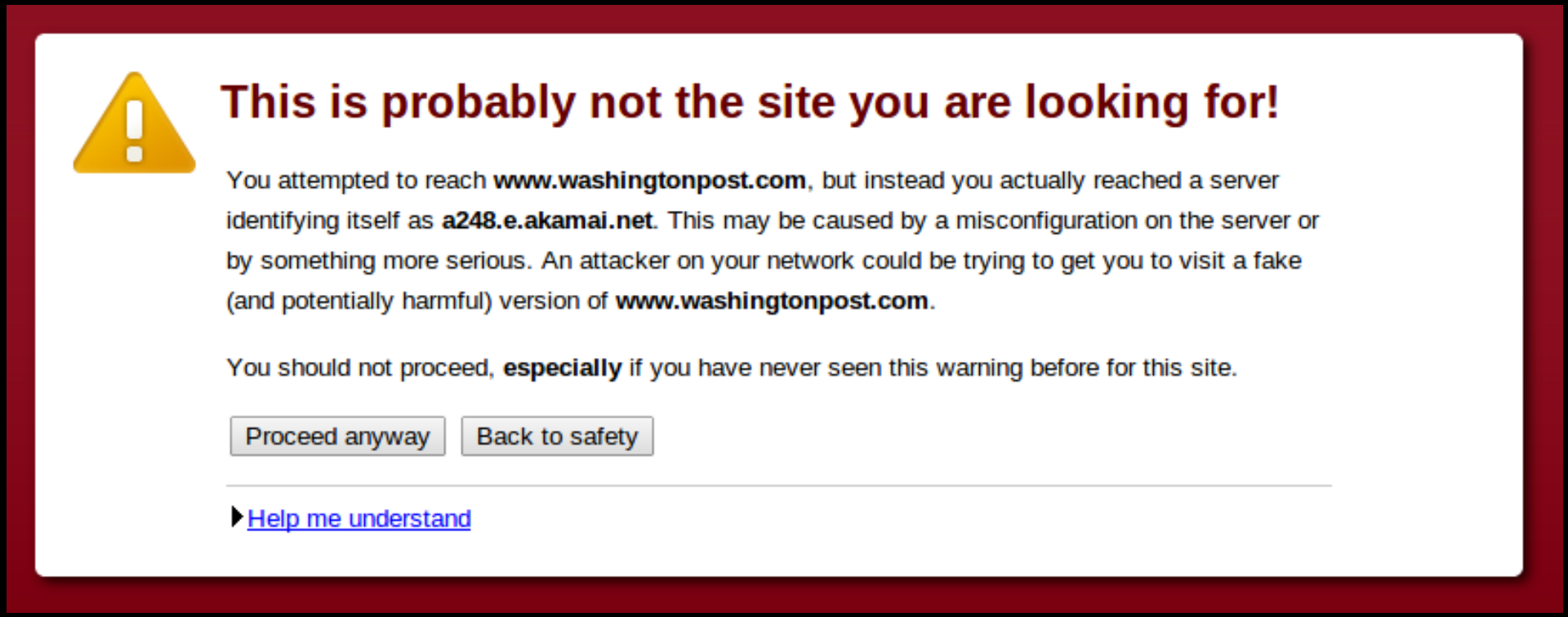
Man in the Middle Attacks (Woman in the Way?)



Certificate Authorities (CAs)

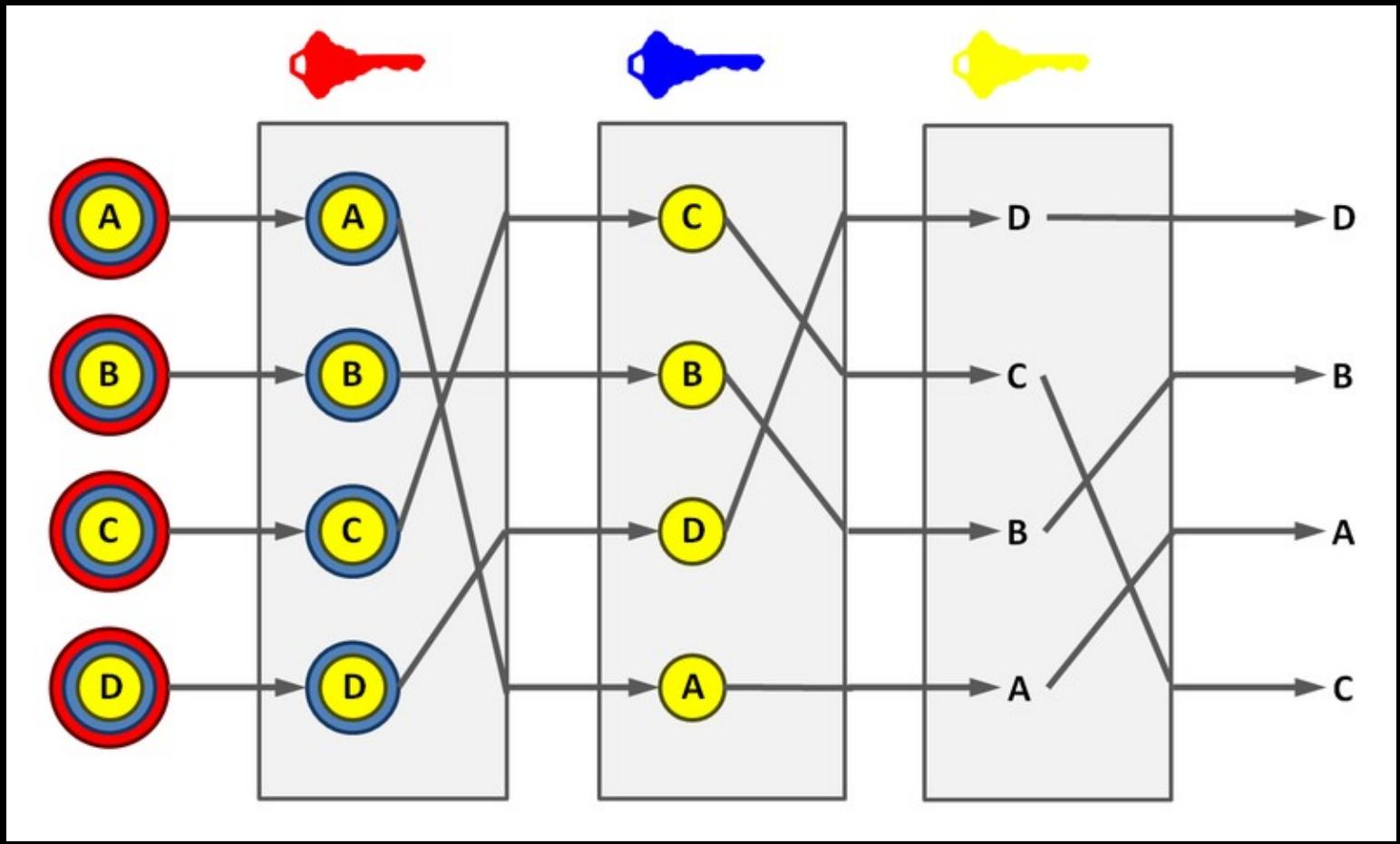
- When you load an HTTPS website it gives you its certificate, which includes its public key
- Your web browser uses this public key to initiate a secure session
- What if there's a MITM attack and you get a malicious public key instead?!
- CAs are companies whose job is to verify that the public key you get is valid

Certificate Authorities (CAs)

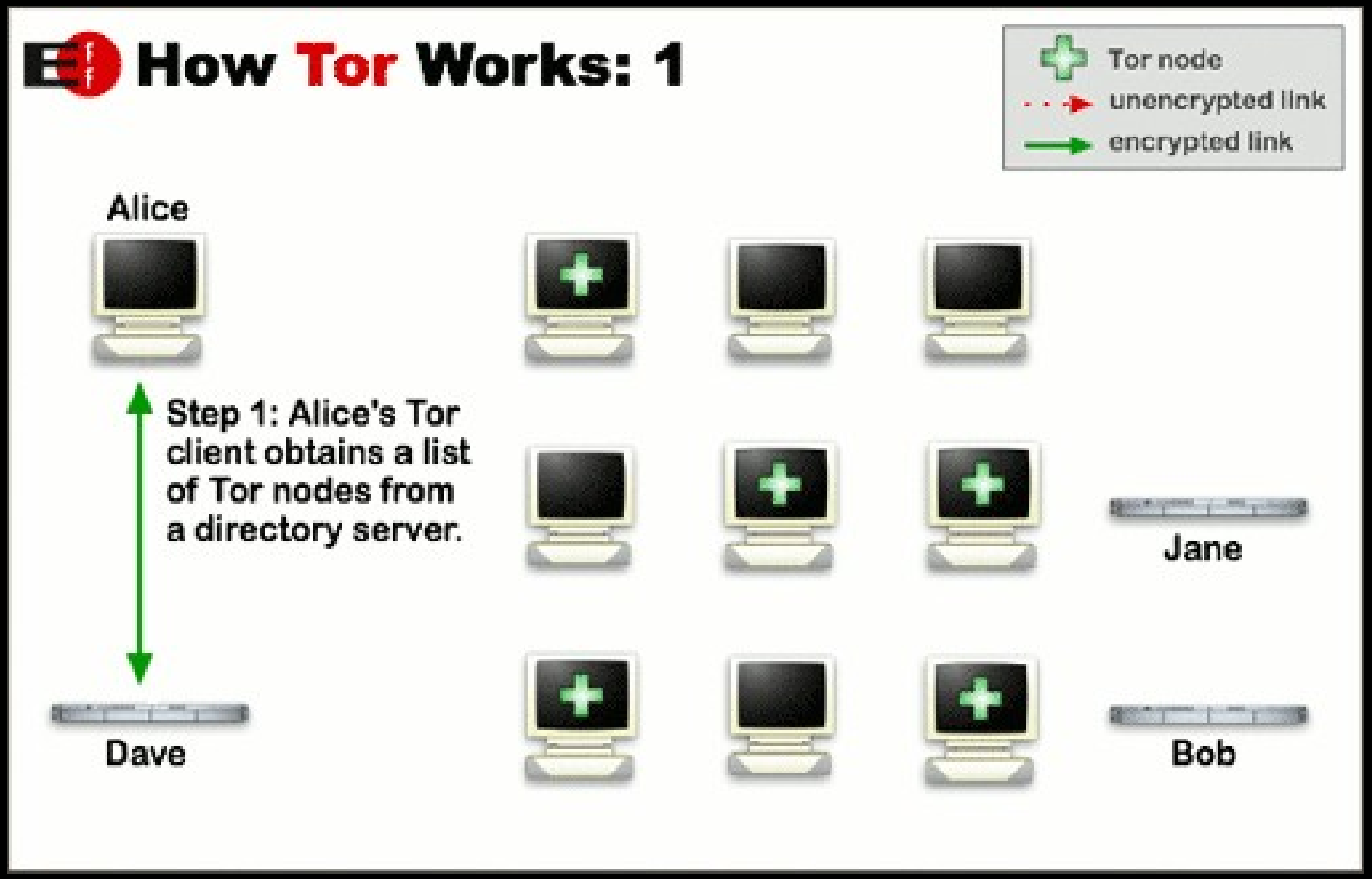


Mix Networks

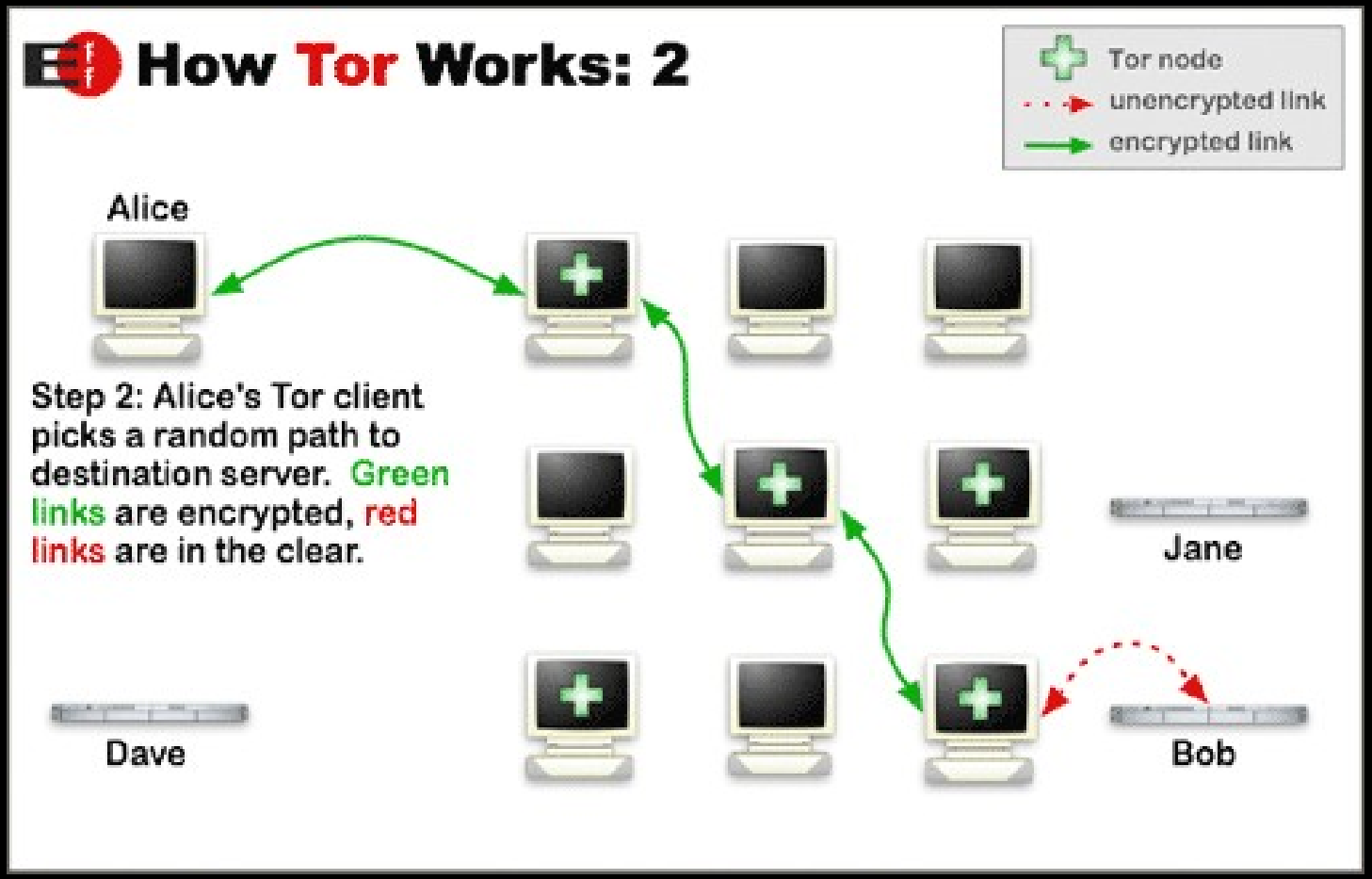
Anonymous Remailers



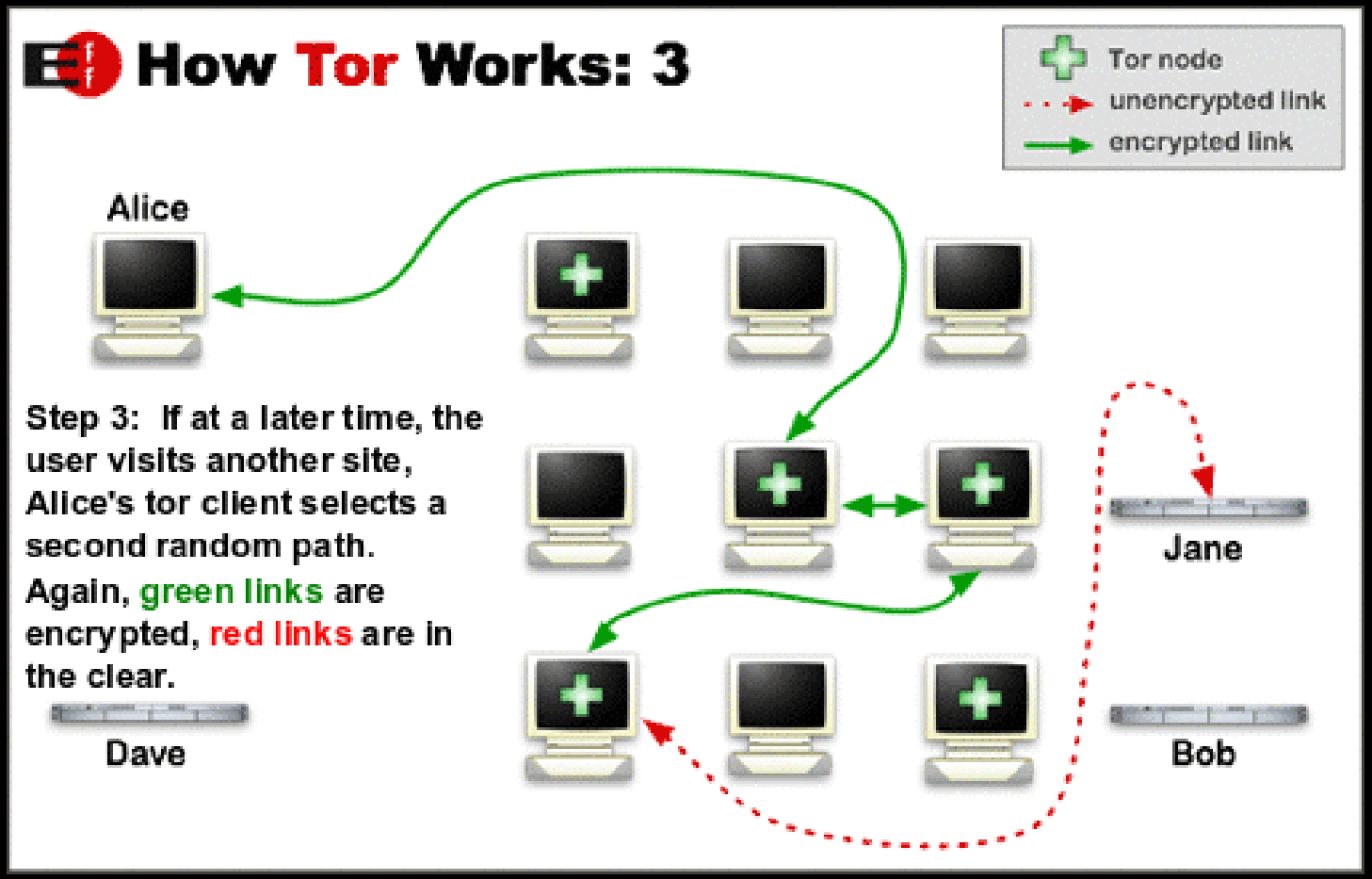
Tor: The Onion Router



Tor: The Onion Router



Tor: The Onion Router



Tor is Easy to Use

Download the Tor Browser from:
https://www.torproject.org/

Use Crypto Today
Off-the-Record IM Encryption

- End-to-end encryption chat over any existing service (Google Talk, Facebook, Jabber, AOL, etc.)
- Windows & Linux: Pidgin and OTR plugin
  https://pidgin.im/
  https://otr.cypherpunks.ca/
- Mac: Adium
  https://adium.im/
- iOS, Android: ChatSecure

Use Crypto Today
Full Disk Encryption

- If you leave your laptop on the bus, your can still remain safe!
- Windows: TrueCrypt, BitLocker
  http://www.truecrypt.org/
- Mac: FileVault (built-in)
- Linux: LUKS (built-in)
- Newer versions of Android (built-in)

Learn More

- EFF's Surveillance Self-Defense Guide: https://ssd.eff.org/
- Security in a Box: https://securityinabox.org/
- Encryption Works: https://pressfreedomfoundation.org/encryption-works

Thank You!

Parker Higgins parker@eff.org @xor
PGP: 4FF3 AA1B D29E 1638 32DE C765 9433 5F88 9A36 7709

Micah Lee micah@eff.org @micahflee
PGP: 5C17 6163 61BD 9F92 422A C08B B4D2 5A1E 9999 9697