Everyday Cryptography

Michael F. Herbst
michael.herbst@iwr.uni-heidelberg.de
http://blog.mfhs.eu

Interdisziplinäres Zentrum für wissenschaftliches Rechnen
Ruprecht-Karls-Universität Heidelberg

24 November 2014

Table of Contents

Table of Contents

Why cryptography?

- Global total surveillance
- *selector-based* surveillance

⇒ Responsibility for people around us as well

- Privacy and confidentiality
- Keeping (company) secrets
- Cryptonoise

Why use free software?

Free Software

0. Use the software as you wish
1. Study the program in source and adapt it as you wish
2. Redistribute copies to help your neighbour
3. Distribute modified copies to help the whole community

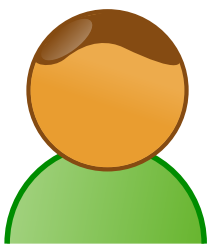
Free Software has higher potential to be secure

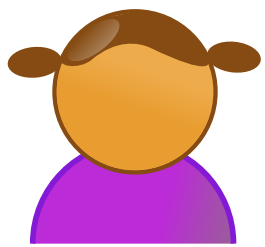
- All Software contains bugs
- Bugs can be fixed by everyone for everyone
- You or person you trust can review source

$\Rightarrow$ Only free software is really trustworthy

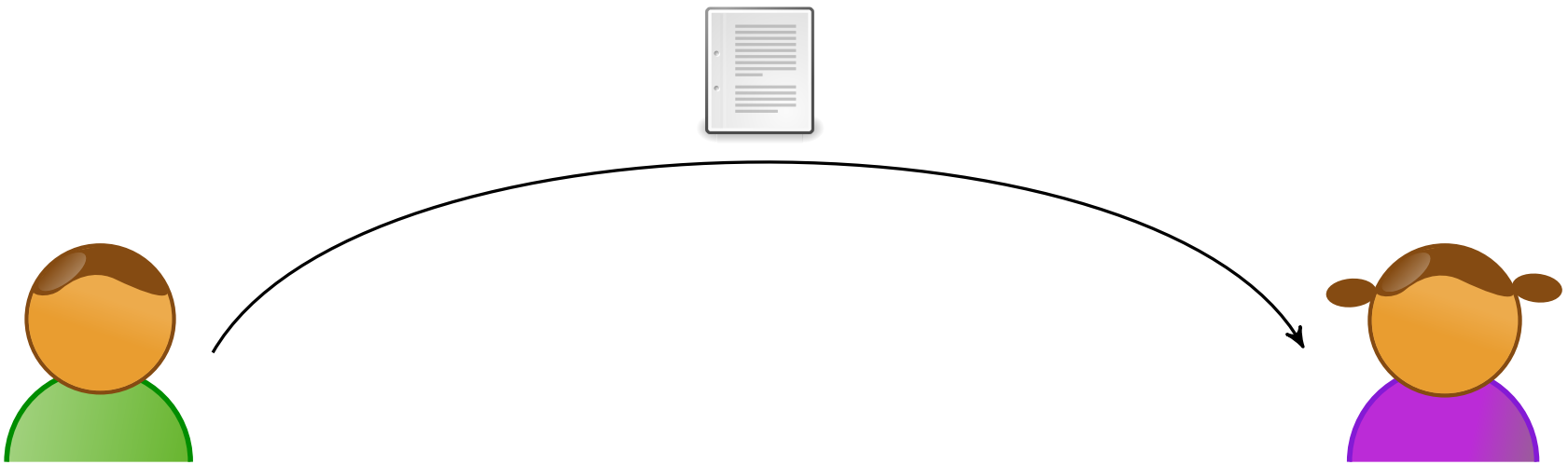
Table of Contents

Unencrypted Emails

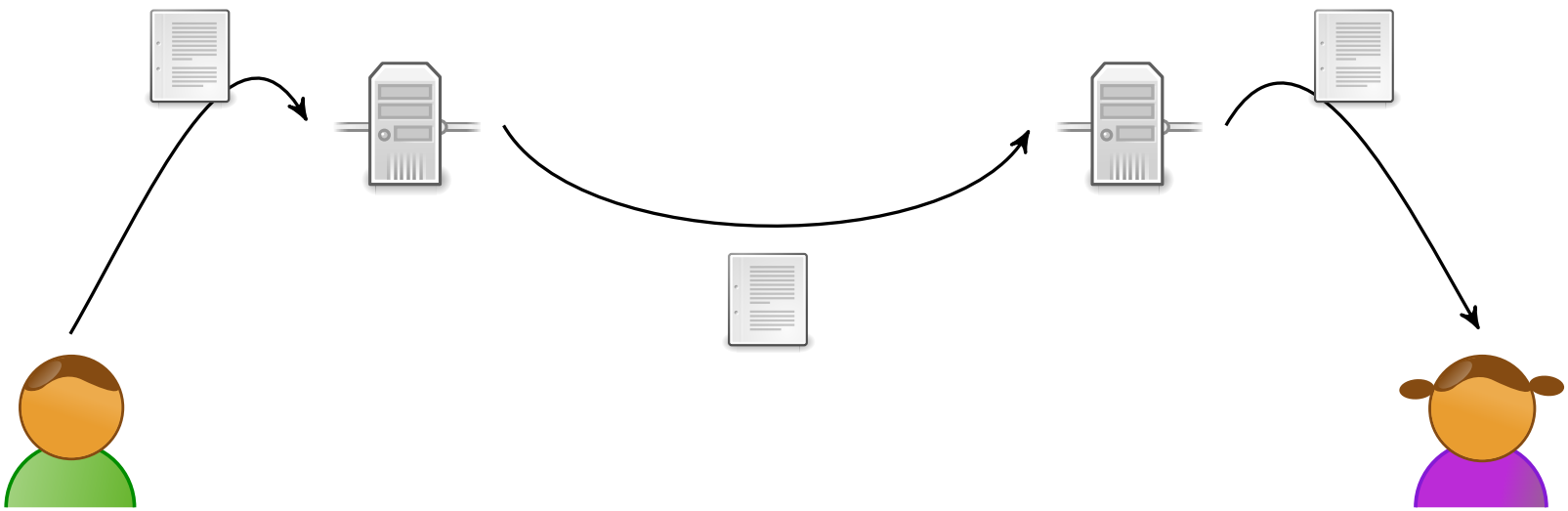




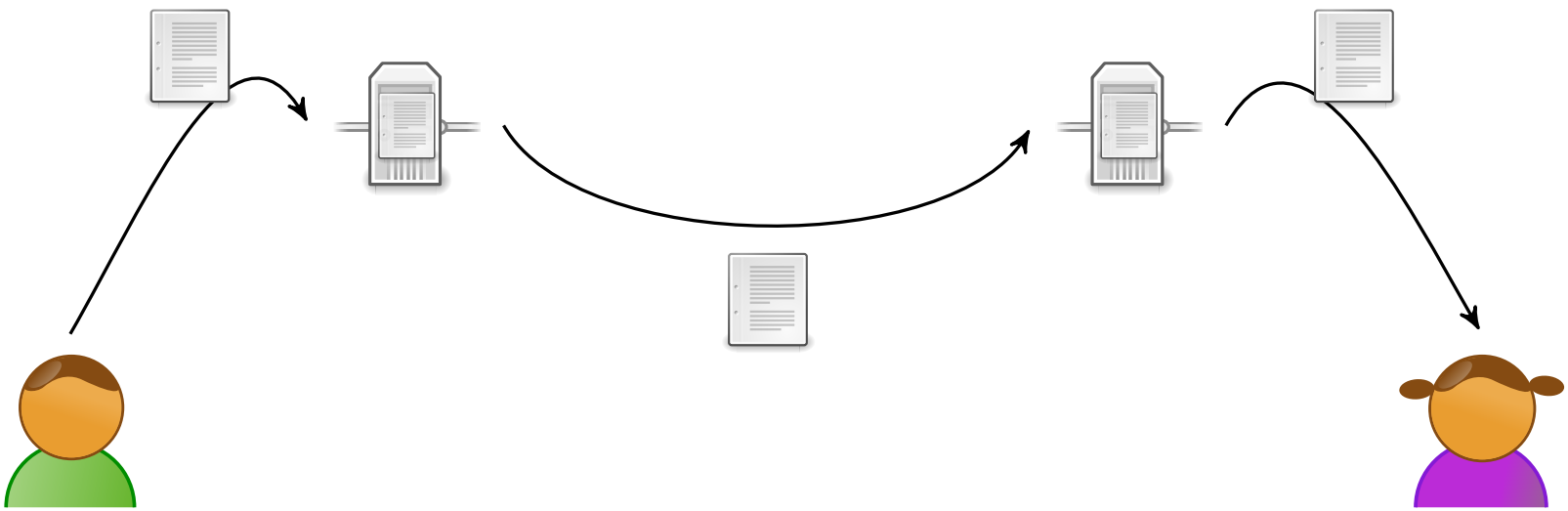
Unencrypted Emails



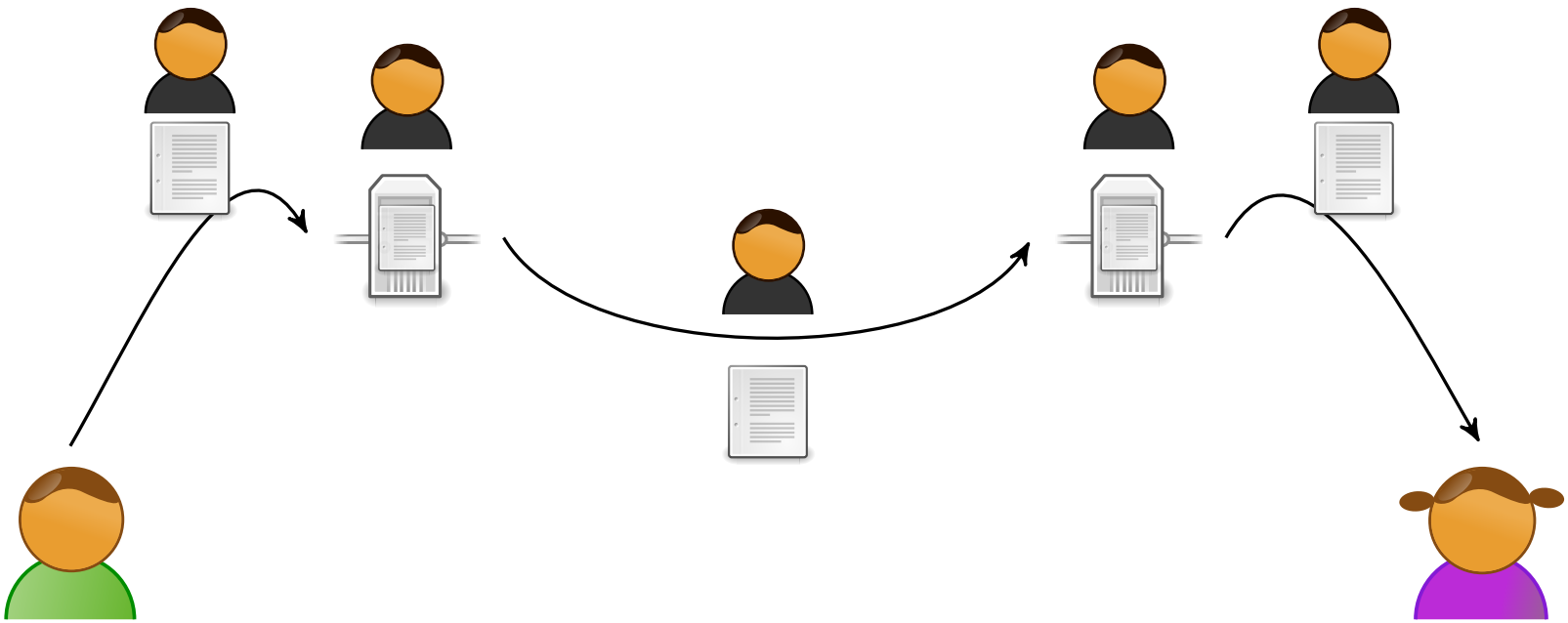
Unencrypted Emails



Unencrypted Emails



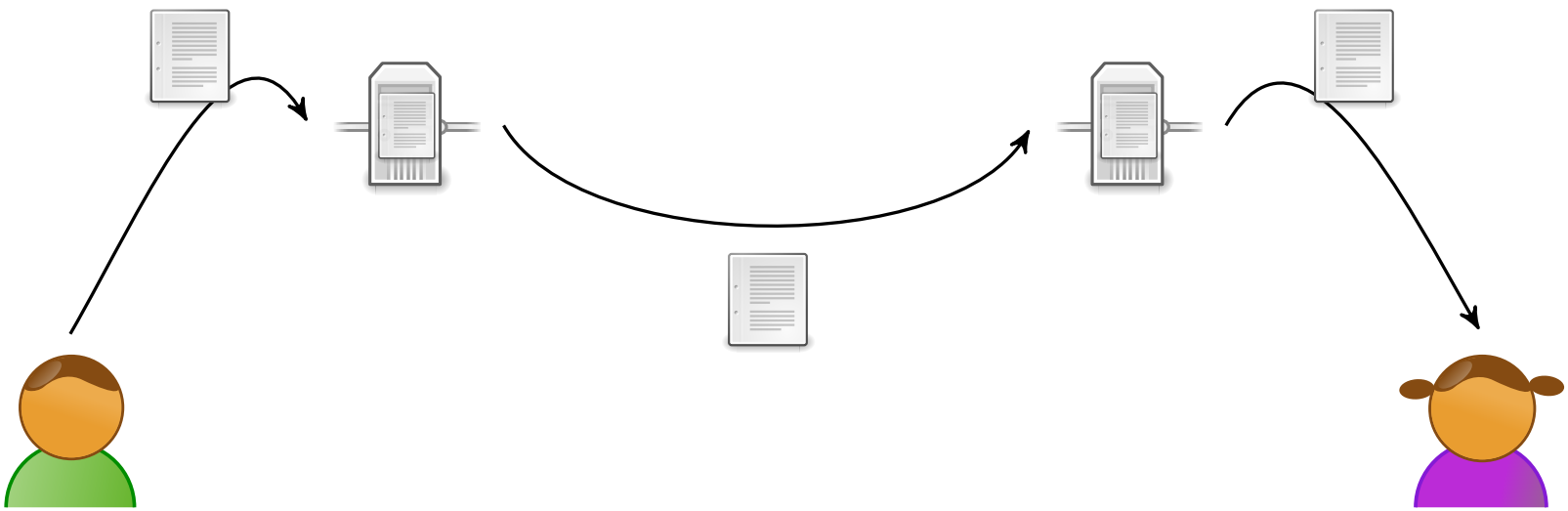
Unencrypted Emails



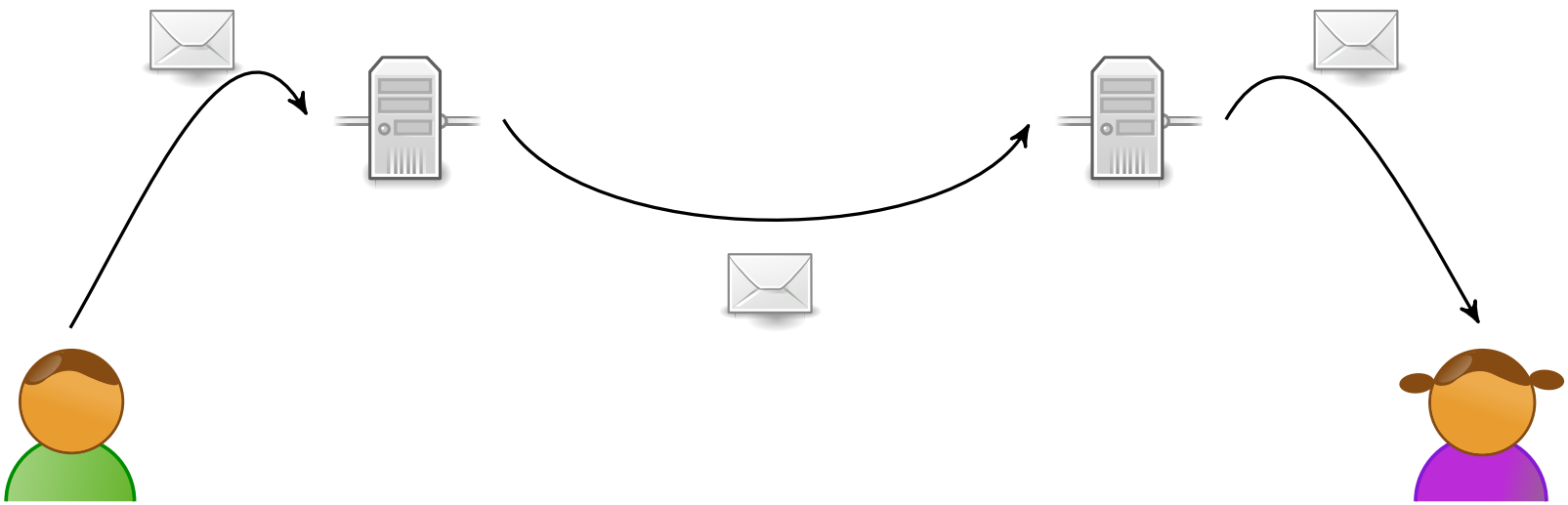
Demo

DEMO

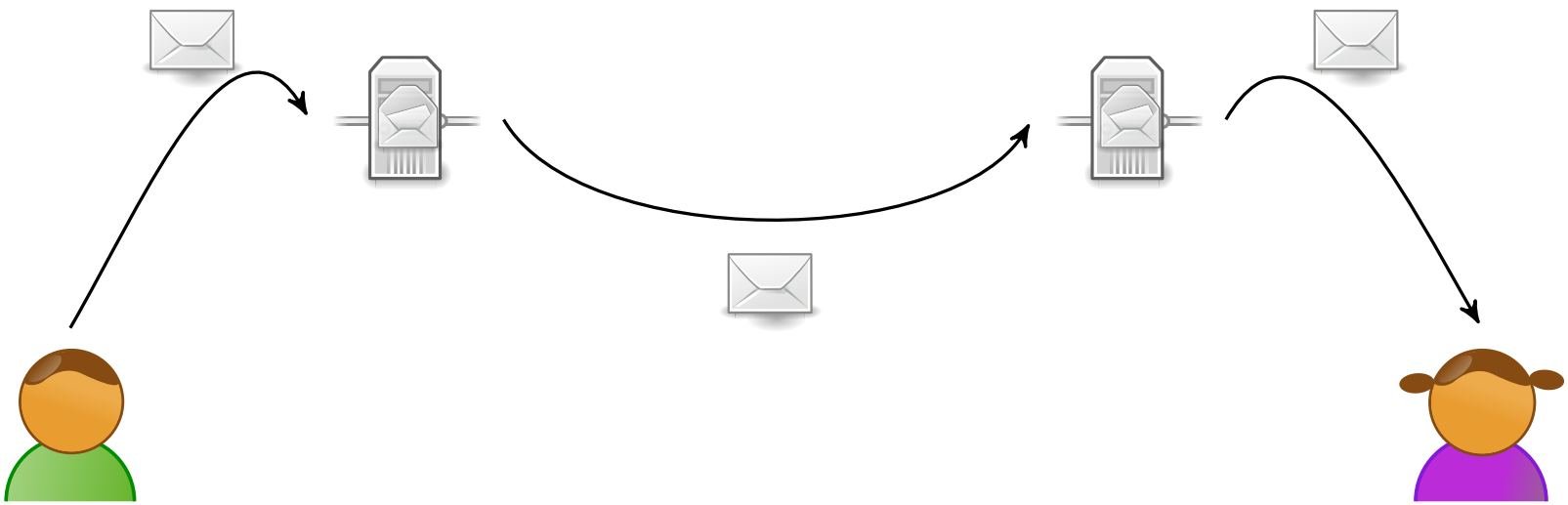
Using Transport Layer Security (TLS)



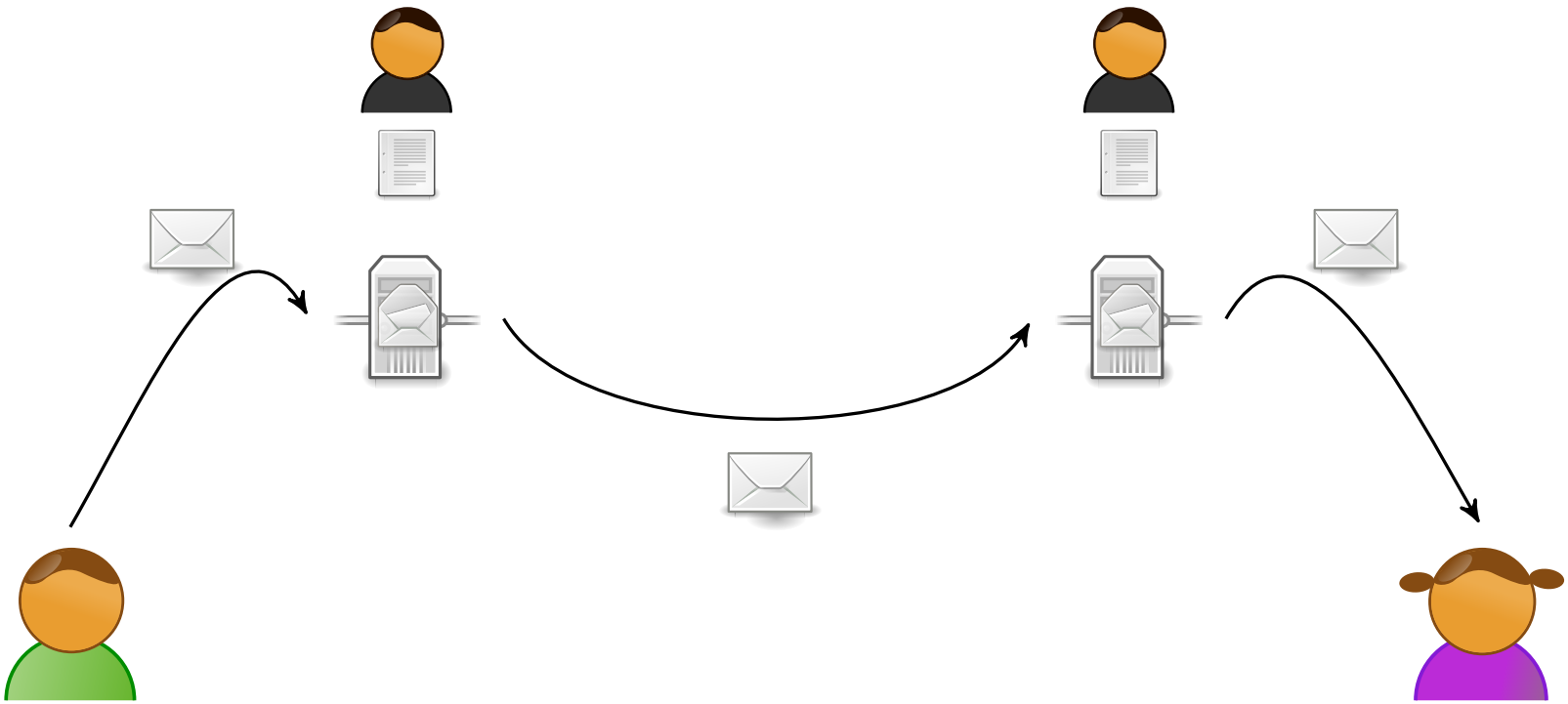
Using Transport Layer Security (TLS)



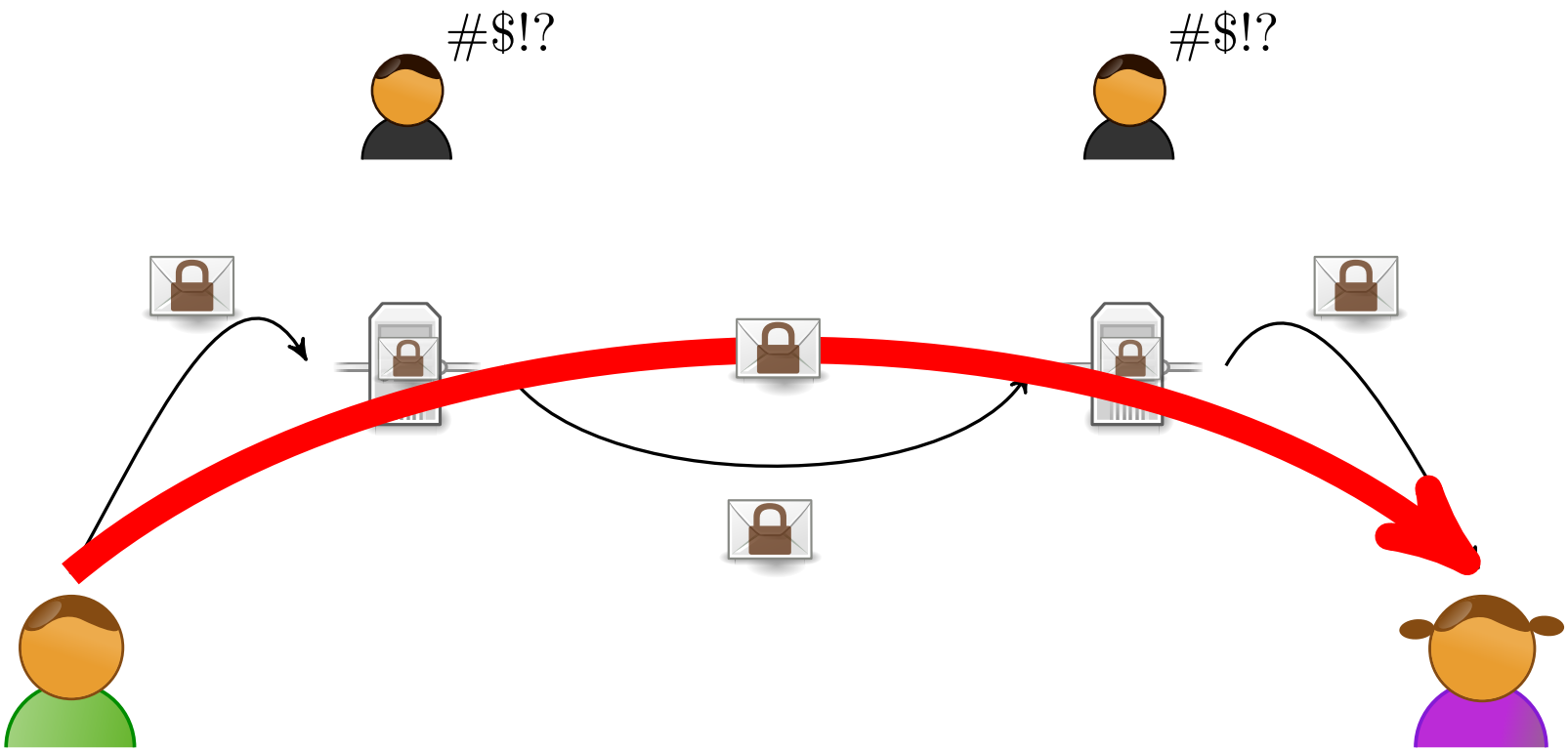
Using Transport Layer Security (TLS)



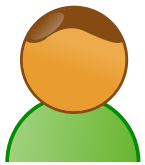
Using Transport Layer Security (TLS)



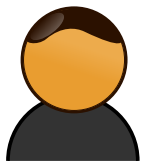
Using End2End encryption (e.g. Pretty Good Privacy)



Asymmetric encryption (here: PGP)

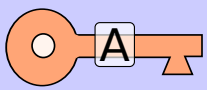


Bob's computer

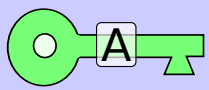


Eve and the internet

Alice's computer

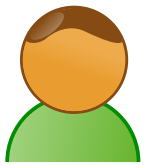


Alice's Private Key

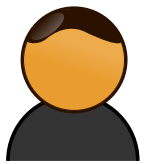


Alice's Public Key

Asymmetric encryption (here: PGP)

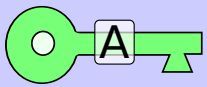


Bob's computer

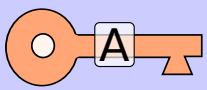


Eve and the internet

Alice's computer

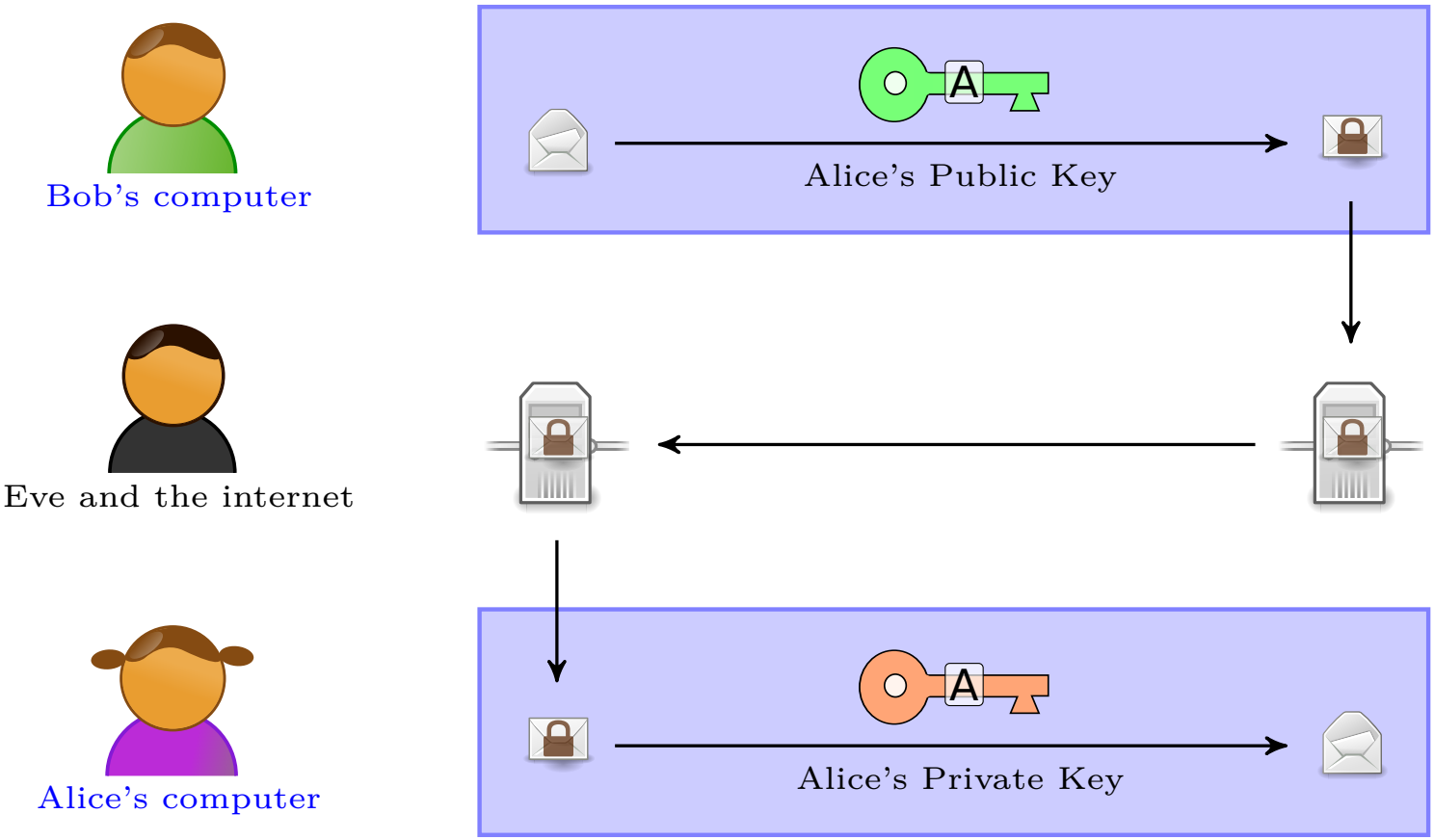


Alice's Public Key

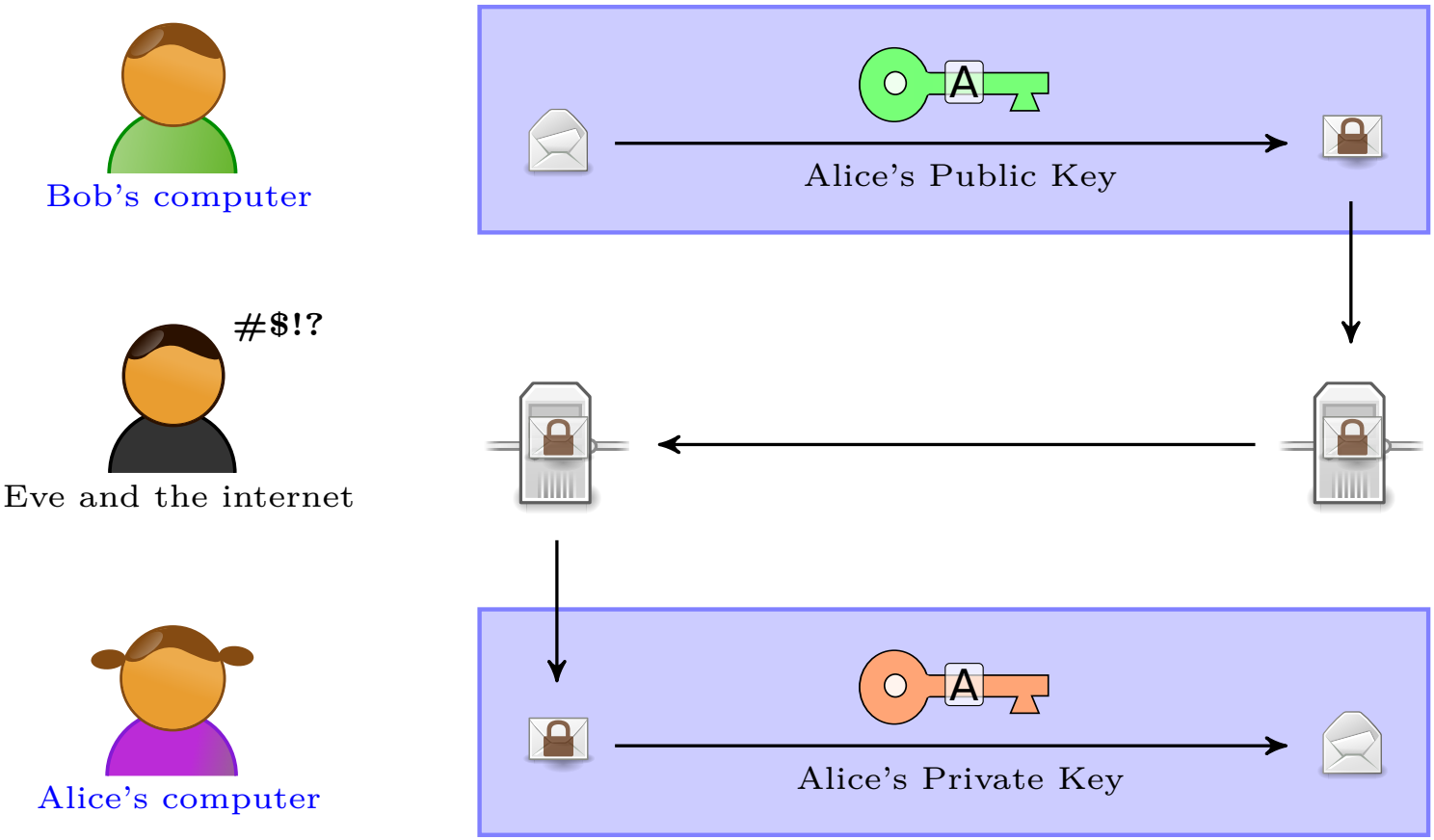


Alice's Private Key

Asymmetric encryption (here: PGP)



Asymmetric encryption (here: PGP)



What do you need?

Programs

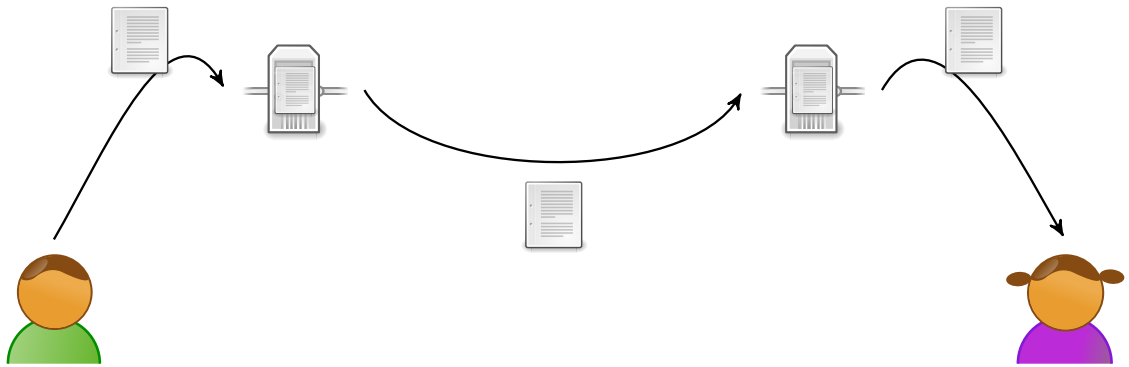
- Thunderbird and Enigmail (Windows, LinuX, OS X)
- GPGTools (OS X with Apple Mail)
- They all use: GnuPG

Links

- `https://www.mozilla.org/thunderbird/`
- `https://www.enigmail.net`
- `https://gpgtools.org/`
- `https://www.gnupg.org/`

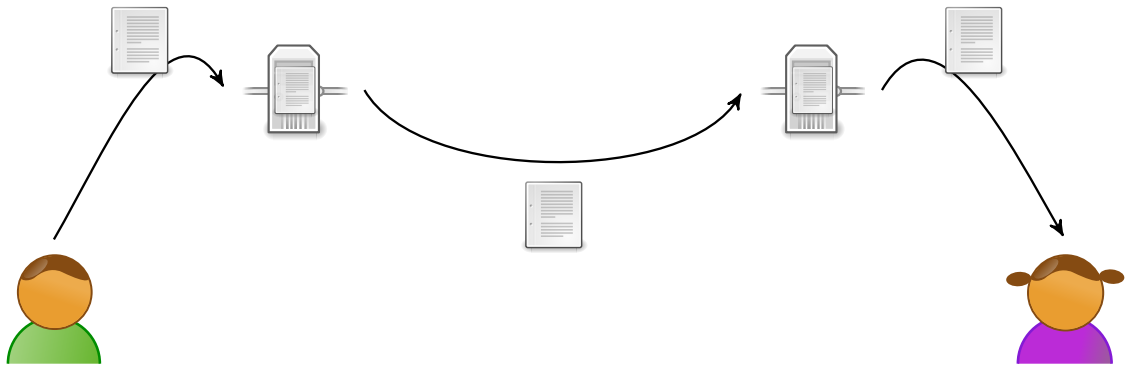
Instant Messaging: Typical setup

Without any encryption

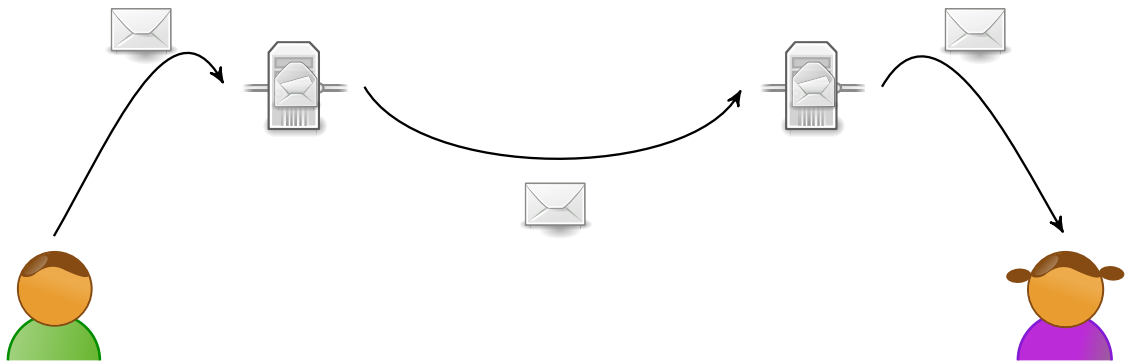


Instant Messaging: Typical setup

Without any encryption



With TLS encryption



Secure Instant Messaging

Protocol

- Asymmetric encryption
- Off-the-record (OTR) messaging — `https://otr.cypherpunks.ca/`
- Works with many chat protocols and everyone who has plugin
- Perfect forward secrecy
- Can establish secret connection via passphrase and other channel

Programs

- Multiprotocol: Facebook chat, Google Talk, SIP, XMPP (Jabber), IRC, MSN, ...
- Adium — `https://www.adium.im/` (OS X)
- Pidgin — `https://pidgin.im/` (Windows, LinuX)
- Jitsi — `https://jit.si/` (Windows, LinuX, OS X)

Secure Video Chats

- Jitsi (`https://jit.si/`) not only good for chatting
- Open source Skype alternative
- Uses End2End *encrypted* video and audio
- Relatively new project (buggy, some pitfalls)
- Aims to be easy-to-use and *secure-by-default*

Table of Contents

Hardware vs. software encryption

Hardware encryption Crypto built-in to hard-drive / chip

Software encryption Crypto realised by program running

- Both can be totally transparent to user
- Both can be attacked if physical access
- Attacking hardware encryption a little easier (warm-replug-attacks)
- Hardware-encryption less portable

$\Rightarrow$ Software encryption almost always the better choice

Warm-replug-attack

- `https://events.ccc.de/congress/2012/Fahrplan/events/5091.en.html`

Software encryption software

LinuX

- dm-crypt and LUKS (package: `cryptsetup`)
- `https://code.google.com/p/cryptsetup/`
- Transparent crypto layer

Windows and OS X

- TrueCrypt 7.1a (not the 7.2 Version)
- Important: Use this link
  `https://www.heise.de/download/truecrypt.html`
- (VeraCrypt — use with care)

Software encryption software

LinuX

- dm-crypt and LUKS (package: `cryptsetup`)
- `https://code.google.com/p/cryptsetup/`
- Transparent crypto layer

Windows and OS X

- TrueCrypt 7.1a (not the 7.2 Version)
- Important: Use this link
  `https://www.heise.de/download/truecrypt.html`
- (VeraCrypt — use with care)

Table of Contents

Summary

- By default everyday communication cannot be considered secure
- Crytpographic alternatives exist
- Setting up crypto initially is a barrier
- Once it runs properly: Almost no extra effort needed
- Regain privacy and trust

Need any help?

- Go to a cryptoparty
- e.g. `http://cryptoparty-hd.de`
- You can give me your email and I'll let you know when the next one happens

Images

- From `https://en.wikipedia.org/wiki/File:Asymmetric_cryptography_-_step_2.svg`

- From the Tango Icon Theme — `http://tango.freedesktop.org`

- The rest is my own work or derived of one of the above
- All released under CC by-sa 4.0

Links

- `https://jit.si/`
- `https://www.enigmail.net`
- `http://cryptoparty-hd.de`
- This presentation will soon be on `http://blog.mfhs.eu`