



# CRYPTO PARTY

...duh!

Wer sind wir?



# Warum?

- Anlasslose Totalüberwachung
- Wahrung der Privatsphäre
- Wahrung der Vertraulichkeit
- Wahrung von Geschäftsgeheimnissen
- Streuen von Cryptonoise

# E-Mail heute

Oder: Was'n das Problem?



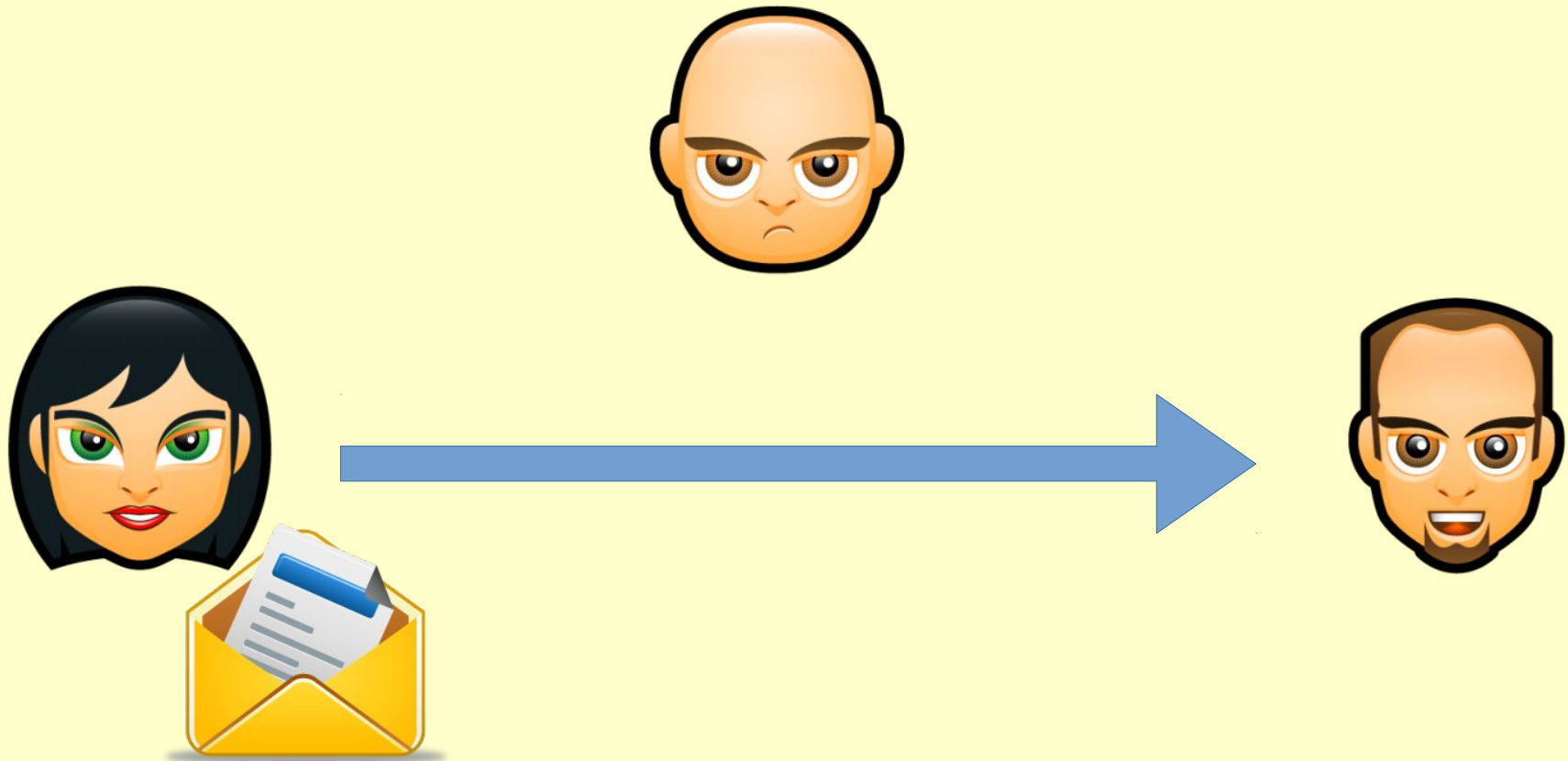




Lorem ipsum dolor sit amet, consectetur adipiscing elit. Mauris sit amet  
Hincidunt ipsum. Namque ante. Pellentesque consetetur donec vel donec  
Suspendisse lectus. Doneque malesuada nulla sed justo velitque pulvinar  
Cras amet ipsum, phasellus et nulla pulvinar, nec vel. Donec sit  
paris. Sed a lorum et vel facilisis consetetur. Integer necessest. Mauris  
et massa vestibulum sed facilisis viverra. Sed fringilla. Nam in lorum et  
lacinia rhoncus sagittis. Sed fringilla. Praesent tempus, tempus vel  
consectetur hendrerit, lacinia et porttitor ligula, nec consetetur sed vel et  
id. Prae diam magna, tempus vitae, lacinia et, viverra id, felis. Nam  
malesuada sapiens et nibh. Fusce venenatis ligula in justo in tempus oris.

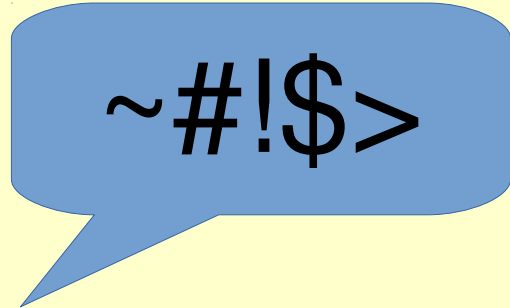
Fusce justo ante, vestibulum vel, rutrum et, hendrerit eu, velit. Praesent  
tempus ante, vestibulum eget, oris sed, dignissim id, oris, justo.  
Suspendisse porttitor. Nunc lorum nec, tristique eget, lacinia et, sagittis  
id, velit. Fusce venenatis ligula in justo. Prae lectus oris, venenatis phasellus,  
egressa id, hendrerit nec, oris. Aliquam imperdiet blandit rutrum, lorum  
ipsum donec sit amet, consetetur adipiscing elit. Sed quis elit. Suspendisse  
porttitor. Nulla blandit justo a rutrum. Mauris tempus diam. Nam sed nisi nec  
elit suscipit ultricesque. Vivamus nisi elit, venenatis id, facilisis oris, blandit  
et, nibh. Cras lacinia lorum oris, sagittis vitae, venenatis a, lacinia id, rutrum.  
Aliquam vel nibh, lorum oris, sagittis eget, viverra et, venenatis id,  
leo. Vivamus fringilla. Duis non velit, ultrices et, hendrerit auctor, rhoncus







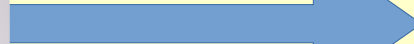


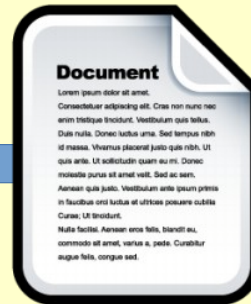
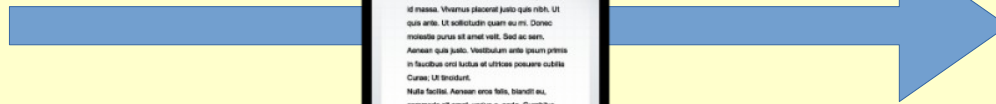


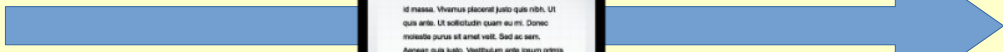
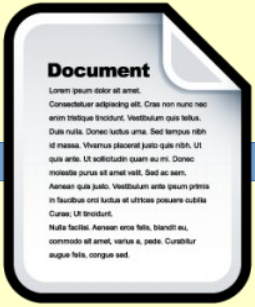


Ut enim ad minim veniam, quis nostrud exercitation ullamco laboris nisi ut aliquip ex ea commodo consequat. Duis aute irure dolor in reprehenderit in voluptate velit esse cillum dolore eu fugiat nulla pariatur. Excepteur sint occaecat cupidatat non proident, sunt in culpa qui officia deserunt mollit anim id est laborum.

Ut enim ad minim veniam, quis nostrud exercitation ullamco laboris nisi ut aliquip ex ea commodo consequat. Duis aute irure dolor in reprehenderit in voluptate velit esse cillum dolore eu fugiat nulla pariatur. Excepteur sint occaecat cupidatat non proident, sunt in culpa qui officia deserunt mollit anim id est laborum.



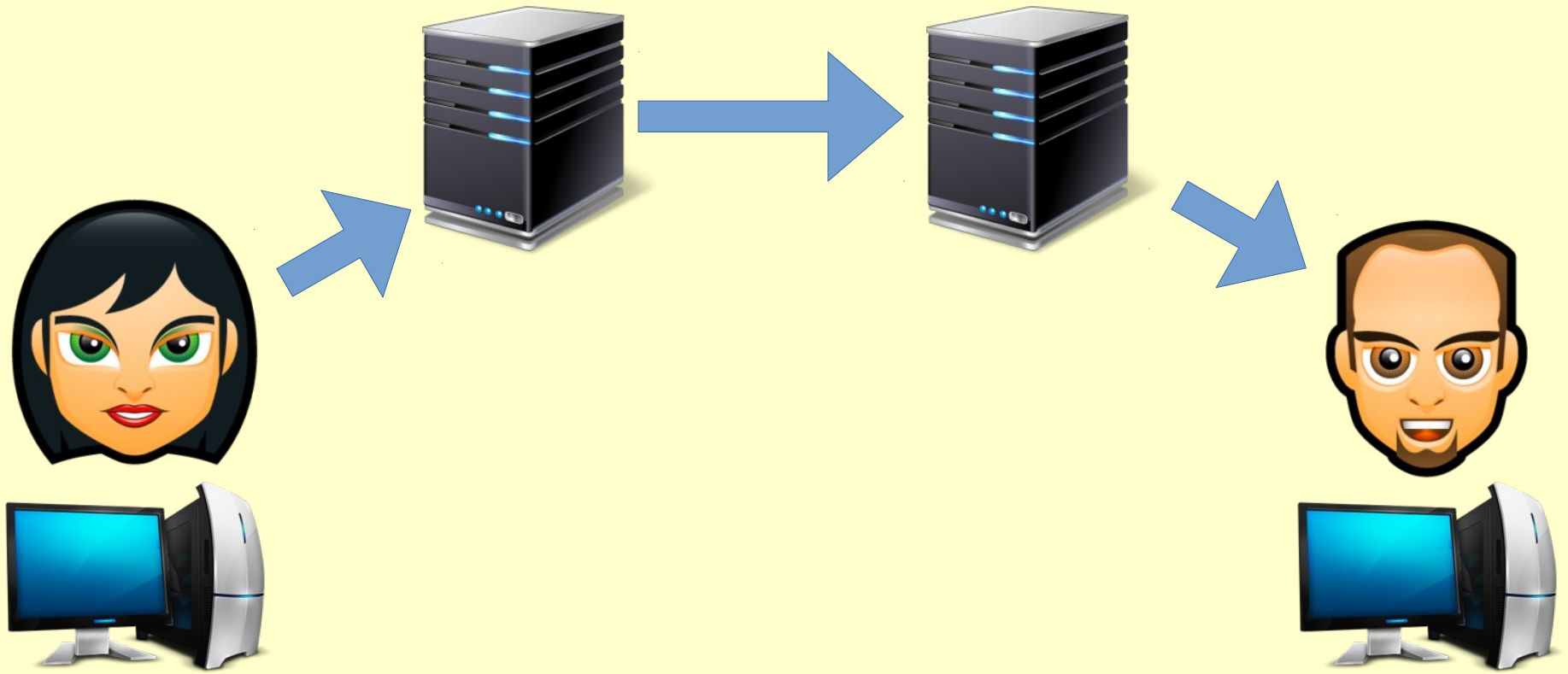


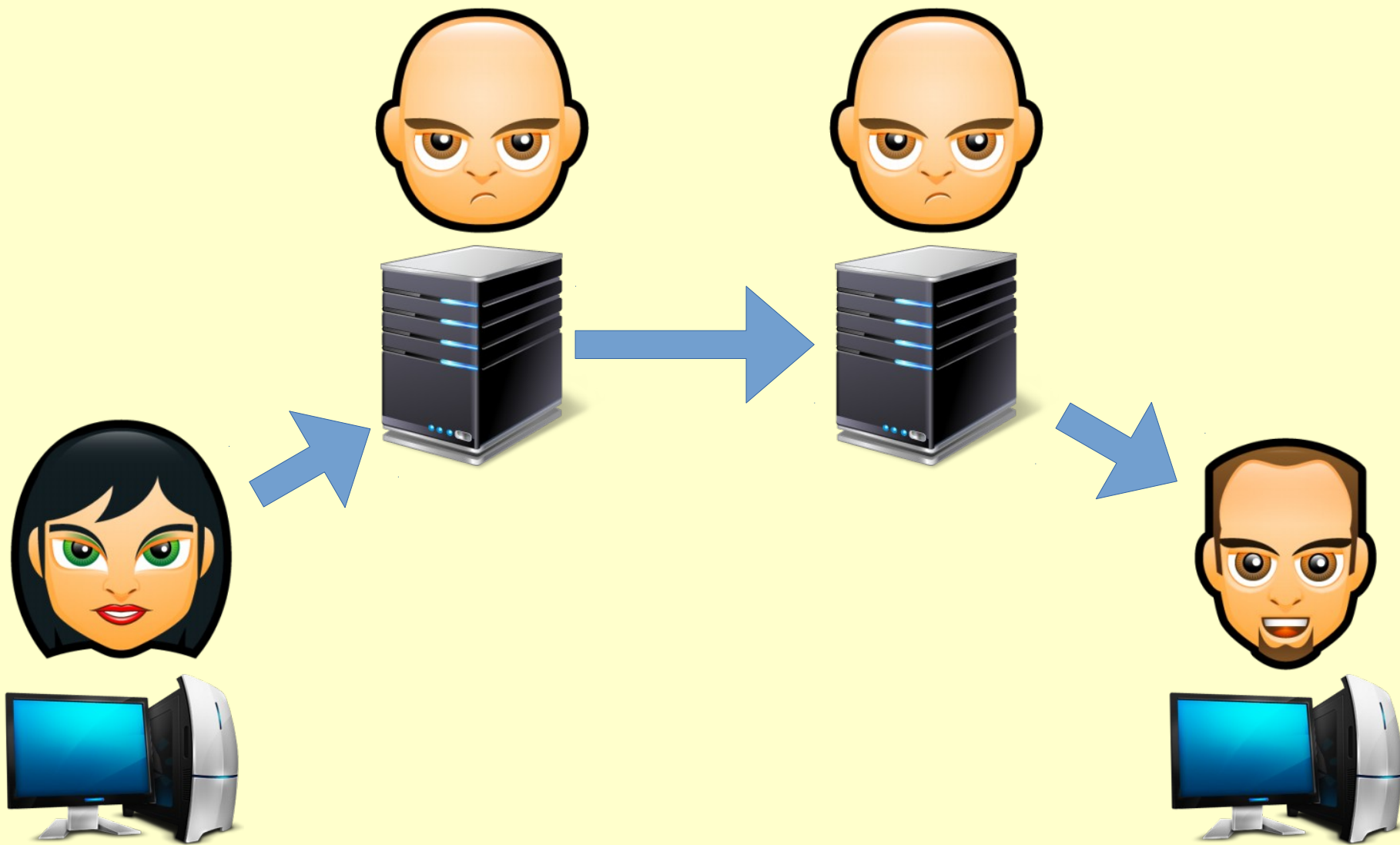




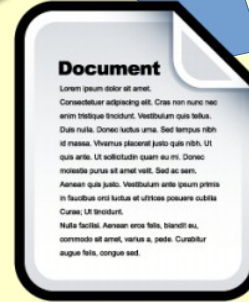
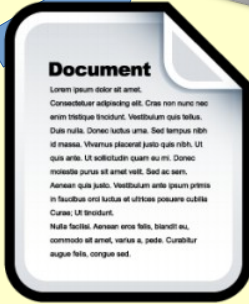
~#!\$>

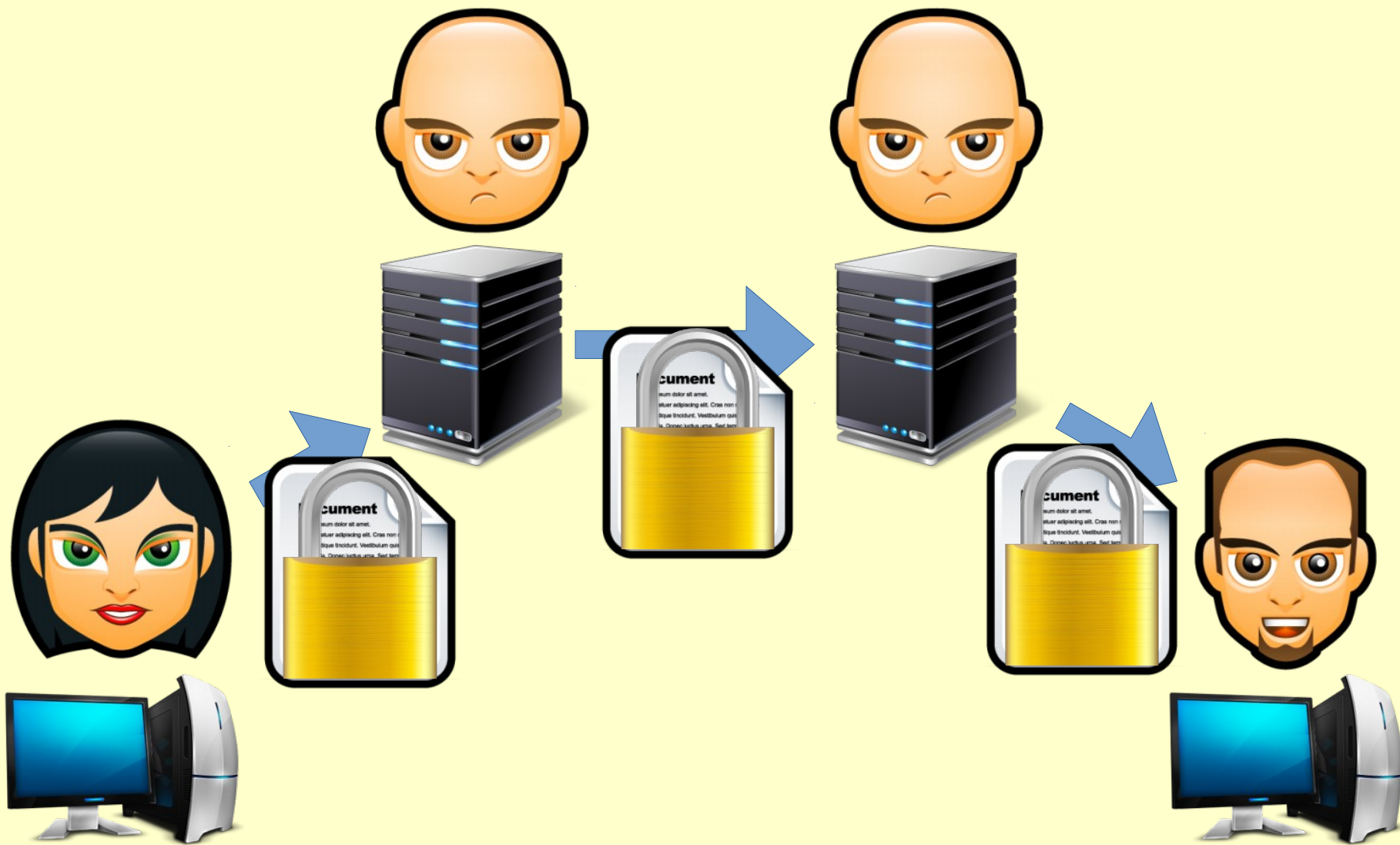




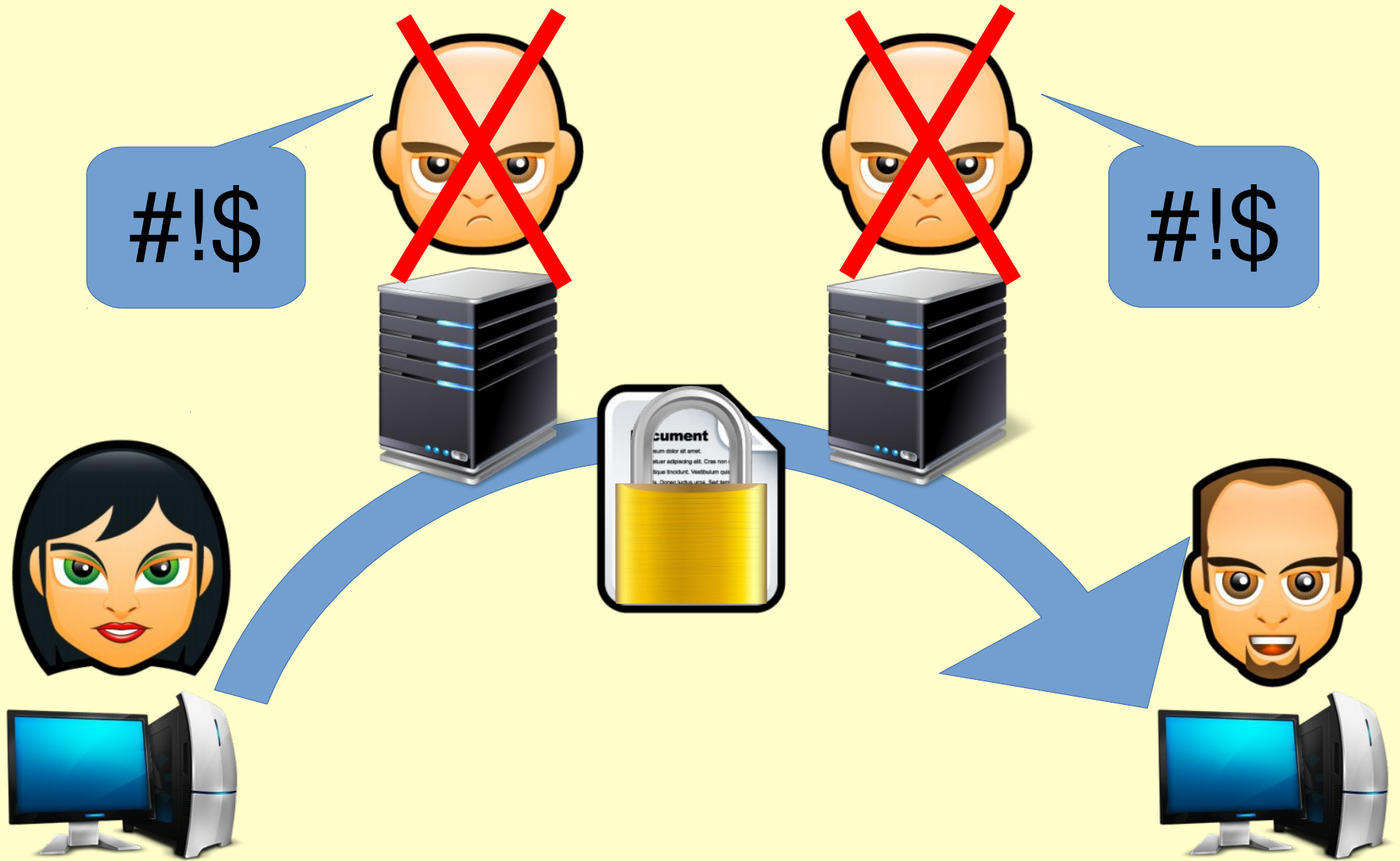








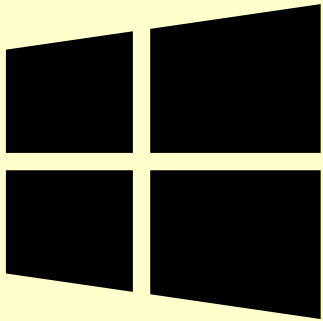
Demo



Demo

Los geht's!

# Ein Mail-Client

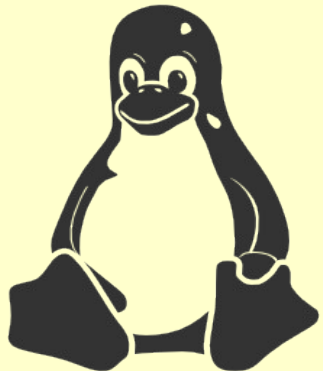


Mozilla Thunderbird

<https://www.mozilla.org/de/thunderbird/>



Apple Mail

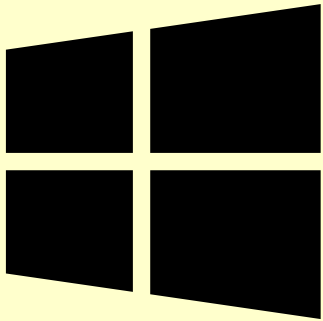


Ubuntu: `apt-get install thunderbird`

Debian: `apt-get install icedove`

...

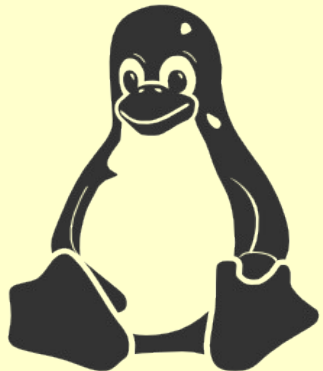
# GnuPG



GPG4Win light  
<http://gpg4win.de/>



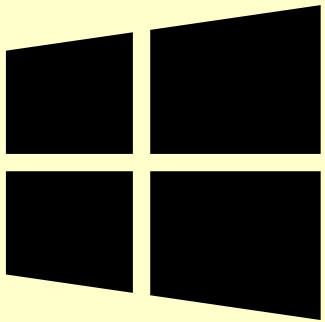
GPG Tools  
<https://gpgtools.org/>



<https://xkcd.com> ;)



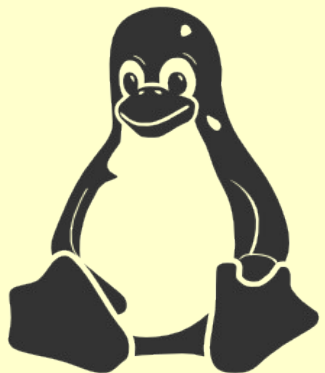
# Integration Mail-Client und GnuPG



Thunderbird Add-On: Enigmail



Nichts zu tun :)



Thunderbird Add-On: Enigmail

Schlüssel erzeugen

Öffentlichen Schlüssel hochladen

[pgp.mit.edu](http://pgp.mit.edu)

Schreibt euch verschlüsselte  
E-Mails!

Oder uns:

[jonas@letopolis.de](mailto:jonas@letopolis.de)

(3B0F5529)

[mail@raphaelmichel.de](mailto:mail@raphaelmichel.de)

(E1C68BA1)

**Aber...**

Demo

Signaturen!

Demo



# Fingerprints

Demo

# Keysigning

Demo

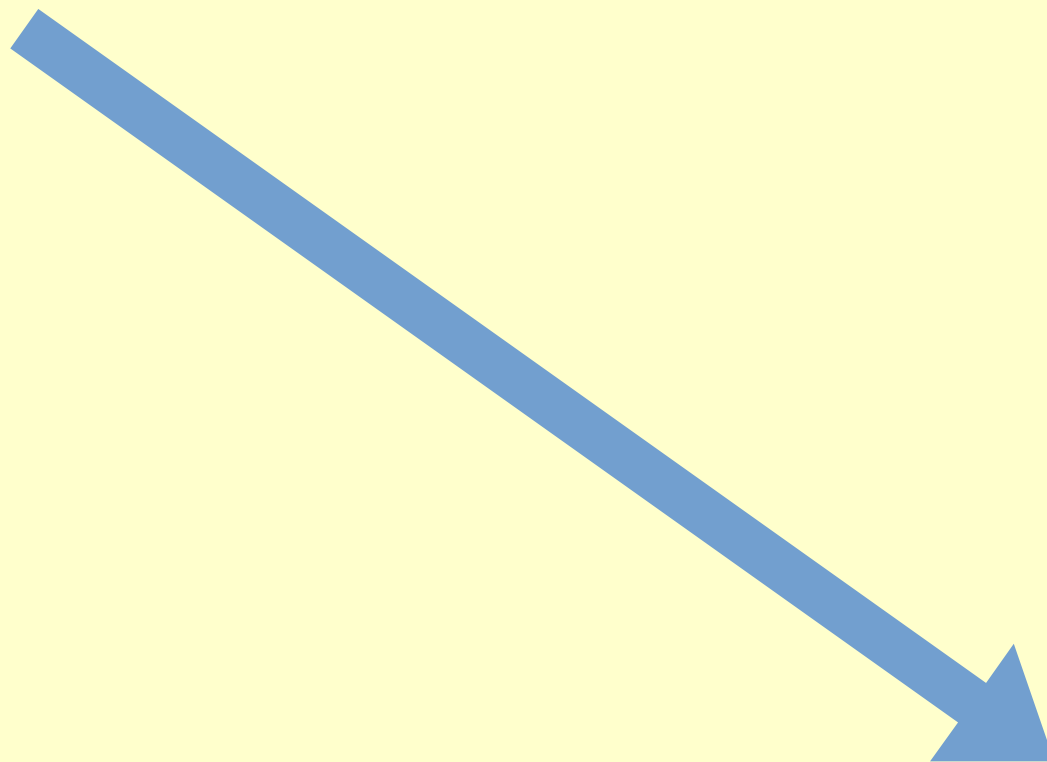
Yay! \o/

# Anonymität

Oder: Muss das jetzt jeder wissen?



89.43.122.65

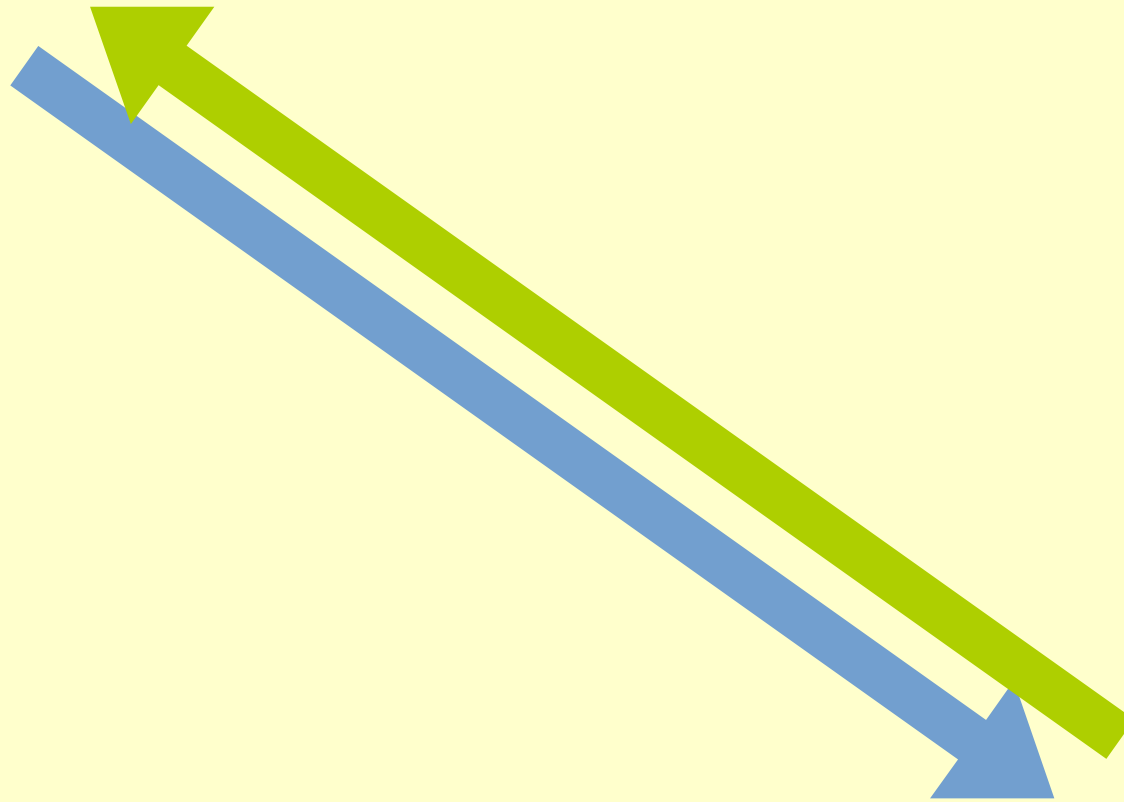


wikipedia.org  
91.198.174.192





89.43.122.65



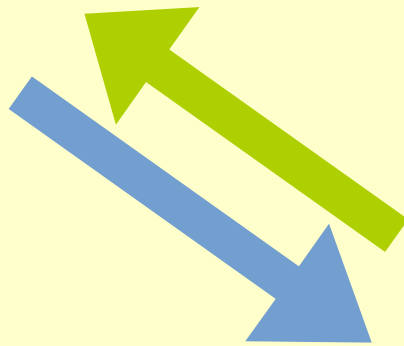
wikipedia.org  
91.198.174.192







89.43.122.65

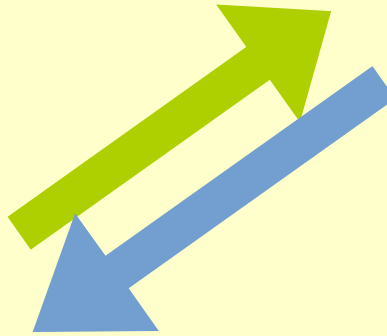
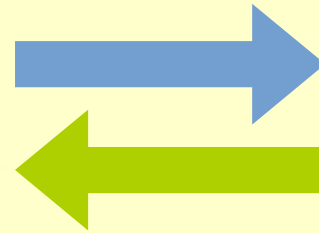
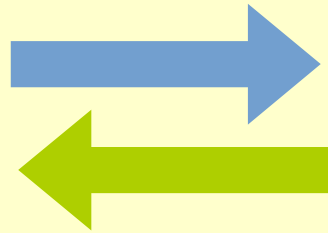


wikipedia.org  
91.198.174.192

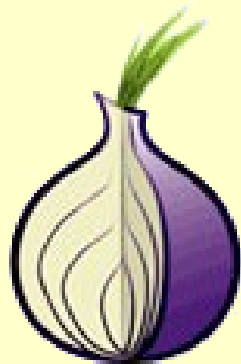




89.43.122.65

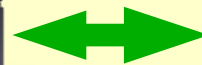
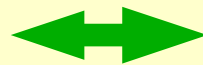
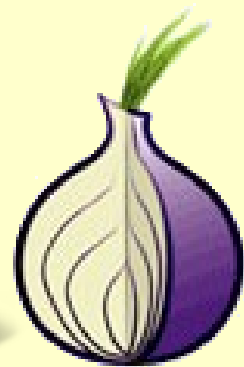


wikipedia.org  
91.198.174.192





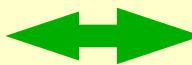
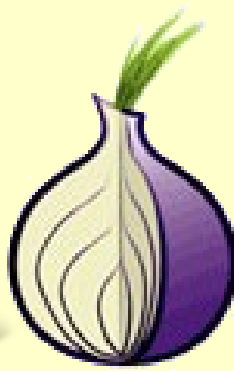
89.43.122.65



wikipedia.org  
91.198.174.192



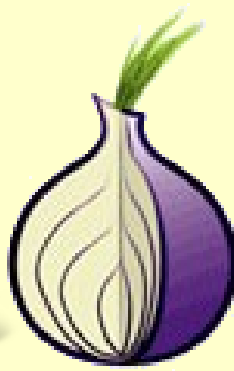
89.43.122.65



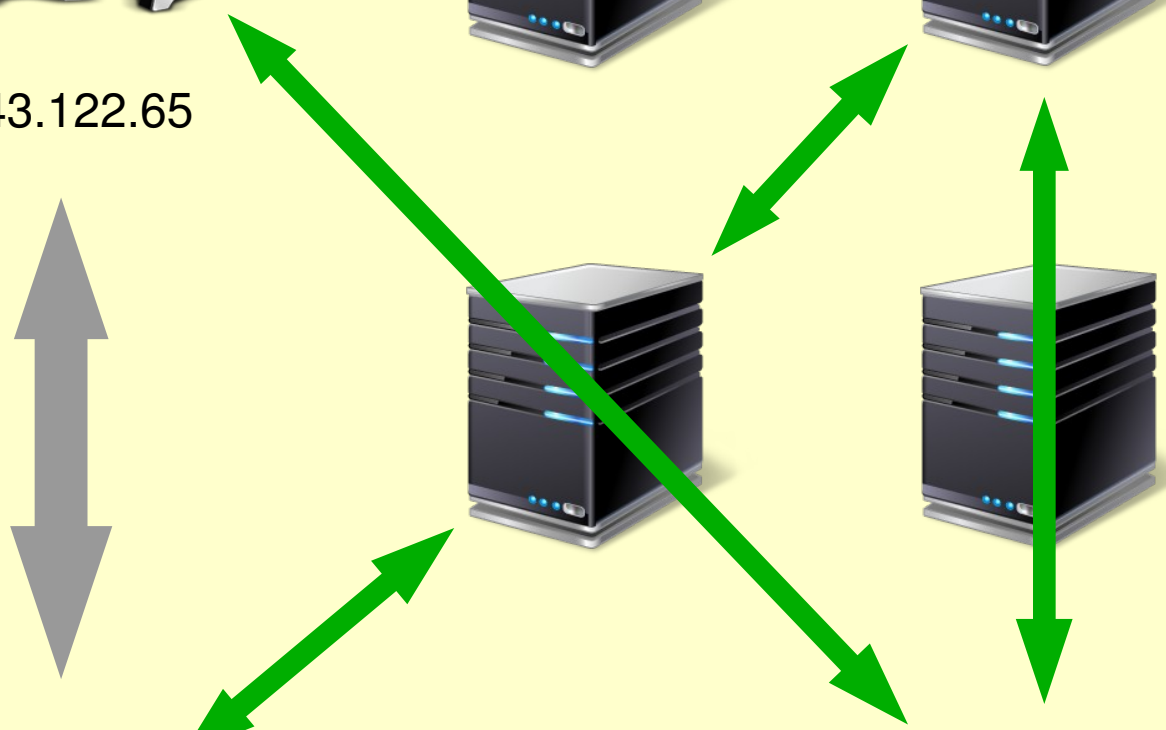
wikipedia.org  
91.198.174.192



89.43.122.65



wikipedia.org  
91.198.174.192



Demo

[torproject.org](https://torproject.org)

# Was gibt's denn sonst noch?

- Verschlüsselung für
  - Dateien & Festplatten
  - Dropbox
  - Messenger & Chat
  - ...
- Möglichkeiten für mehr Sicherheit & Anonymität ohne den Torbrowser



# Was gibt's denn sonst noch?

- Verschlüsselung für
  - Dateien & Festplatten
  - Dropbox
  - Messenger & Chat
  - ...
- Möglichkeiten für mehr Sicherheit & Anonymität ohne den Torbrowser

Aber: die liebe Zeit....



Bei Interesse: fragt uns! :)

Vielen Dank!

Material:

[cryptoparty-hd.de](http://cryptoparty-hd.de)

Alle Angaben ohne Gewähr



<http://www.iconarchive.com/show/face-avatars-icons-by-hopstarter/Female-Face-FC-5-icon.html>



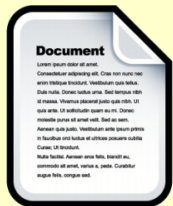
<http://www.iconarchive.com/show/face-avatars-icons-by-hopstarter/Male-Face-F2-icon.html>



<http://www.iconarchive.com/show/real-vista-communications-icons-by-icons shock/clock-icon.html>



<http://www.iconarchive.com/show/emluator-icons-by-jommans/My-Computer-icon.html>



<http://www.iconarchive.com/show/sleek-xp-basic-icons-by-hopstarter/Document-icon.html>



<http://www.iconarchive.com/show/pretty-office-2-icons-by-custom-icon-design/new-message-icon.html>



<http://www.iconarchive.com/show/pretty-office-2-icons-by-custom-icon-design/message-already-read-icon.html>



<http://www.iconarchive.com/show/oxygen-icons-by-oxygen-icons.org/Actions-document-encrypt-icon.html>



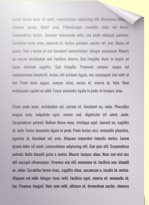
<http://www.iconarchive.com/show/face-avatars-icons-by-hopstarter/Male-Face-A1-icon.html>



<http://www.iconarchive.com/show/vista-hardware-devices-icons-by-icons-land/Home-Server-icon.html>



<http://www.iconarchive.com/show/real-vista-communications-icons-by-icons shock/clock-icon.html>



<http://icons.iconarchive.com/icons/franksouza183/fs/512/Mimetypes-text-plain-icon.png>



<https://www.torproject.org>



EFF, CC-by