

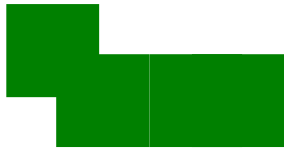
Vorkurs Linux-Grundlagen

Vorkurs Linux / Informatik Tag 3

Heute:

- Operationen auf Prozessen (= Programme)
- Zugriffsrechte von Dateien verwalten
- Dateien suchen und archivieren

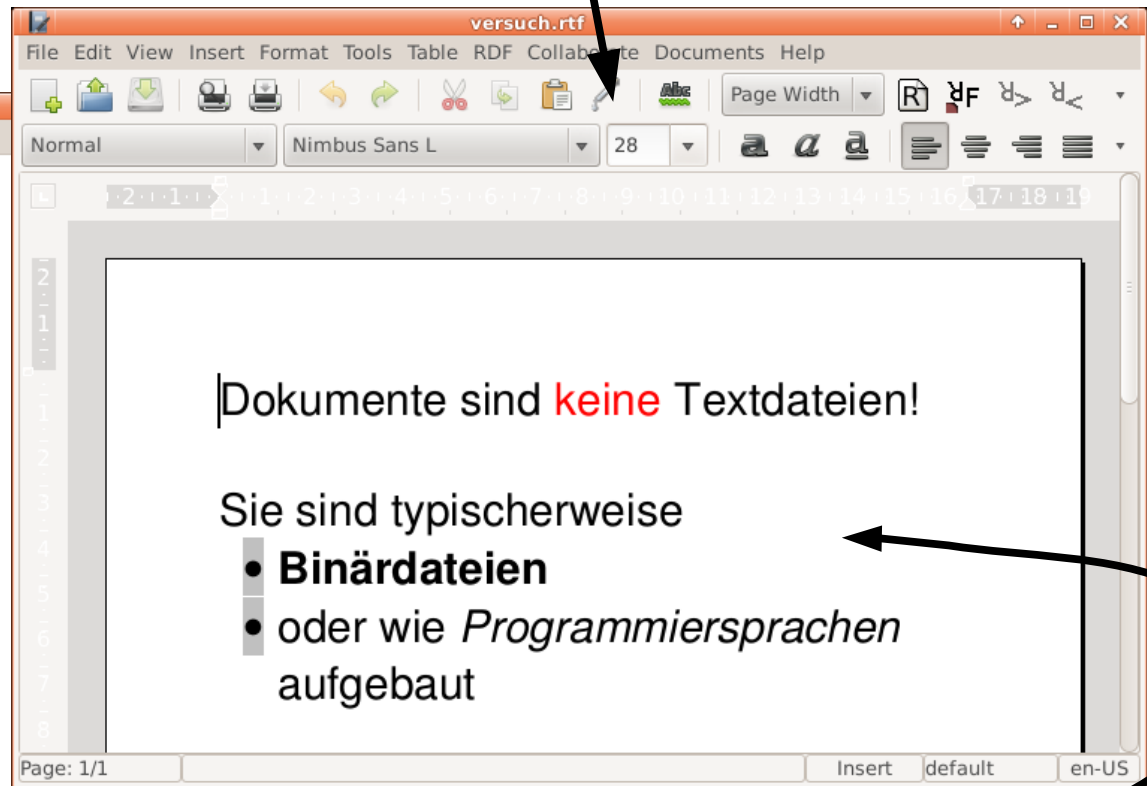
- Grundlagen und Hintergründe zu E-Mail



Wiederholung

Texteditoren \neq Textverarbeitung

```
File Edit Search Options Help
{\rtf1\ansi\ansicpg1252\deff0
{\fonttbl
{\f0\fnil\fcharset0\fpqr0\fttruetype Nimbus Sans L;}
{\f1\fnil\fcharset0\fpqr0\fttruetype Symbol;}
{\f2\fnil\fcharset0\fpqr0\fttruetype Arial;}
{\f3\fnil\fcharset0\fpqr0\fttruetype Dingbats;}
{\f4\fnil\fcharset0\fpqr0\fttruetype Times New Roman;}
{\f5\fnil\fcharset0\fpqr0\fttruetype Courier New;}}
{\colortbl
\red0\green0\blue0;
\red255\green255\blue255;
\red255\green255\blue255;
\red255\green0\blue0;}
{\stylesheet
{\s1\fi-431\li720\sbasedon29\snext29 Contents 1;}
{\s2\fi-431\li1440\sbasedon29\snext29 Contents 2;}
{\s3\fi-431\li2160\sbasedon29\snext29 Contents 3;}
{\s8\fi-431\li720\sbasedon29 Lower Roman List;}
{\s5\tx431\sbasedon25\snext29 Numbered Heading 1;}
{\s6\tx431\sbasedon26\snext29 Numbered Heading 2;}
{\s7\fi-431\li720 Square List;}
{\s12\sbasedon29 Endnote Text;}
{\s22\fi-431\li720 Bullet List;}
{\s4\fi-431\li2880\sbasedon29\snext29 Contents 4;}
{\s10\fi-431\li720 Diamond List;}
{\s11\fi-431\li720 Numbered List;}
{\*\s13\fs20\super Endnote Reference;}
```



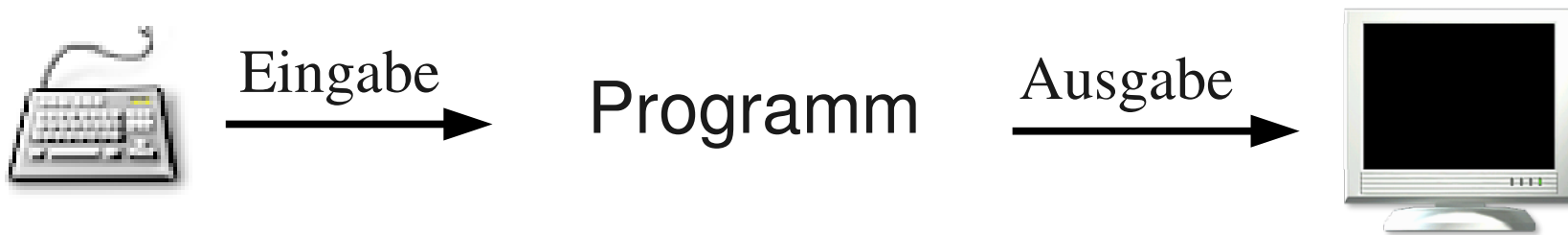
Das steht wirklich in der Datei!

Das seht ihr in AbiWord!



Wiederholung

Ein-/Ausgabeumleitung



Beispiel:

```
4 + 7
9 * 3
quit
```

```
11
27
```

```
> bc < eingabe.txt > ausgabe.txt
```



Wiederholung



Eingabe



Programm₁



Programm₂



...



Programm_n

Ausgabe



```
> ls -l | sort -k 5 -n | less
```



Wiederholung

Verarbeitung von Textdateien

- less
- sort
- cat
- diff
- head, tail
- grep

Texteditor Emacs

Abkoppeln von Programmen mit &



Was machen wir heute?

- Operationen auf Prozessen (= Programme)
- Zugriffsrechte von Dateien verwalten
- Dateien suchen und archivieren

- Grundlagen und Hintergründe zu E-Mail



1. Block: Prozesse

ablaufende Programme = Prozesse

Typische Operationen:

- laufende Prozesse anzeigen
- (unerwünschte) Prozesse beenden



Prozesse anzeigen

[ps](#) - process summary (Unix: Programme→Prozesse)

> **ps**

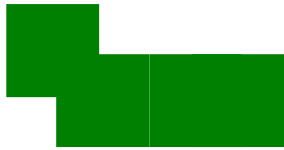
alle Prozesse dieses Kommandozeilen-Fensters

> **ps ux | less**

alle meine Prozesse

> **ps aux | less**

alle Prozesse (auch anderer Benutzer, Systemprozesse)



Prozesse beenden

Abbruch aus der Kommandozeile:

- Ctrl-c oder Ctrl-d (bzw. Strg-c, Strg-d)
- hilft aber nicht immer

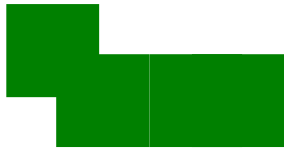
kill – Prozess beenden

- Prozess-ID (pid) mit Hilfe von `ps` ermitteln

> `kill pid` freundliche Version

> `kill -9 pid` unfreundliche Version

- Unix räumt vollständig auf – kein Neustart notwendig!



Laufende Prozesse beobachten

[top](#) : zeige Anfang der Prozess-Warteschlange

> `top`

- Verlassen mit Taste `q`
- laufenden Prozess beenden mit Taste `k`,

dann `pid` und `signal`:

15 für „freundlichen“ Abbruch;

9 für „harten“ Abbruch



Schonender Umgang mit Ressourcen

Unix ist ein Mehrbenutzersystem

→ alle Benutzer konkurrieren um die Rechenzeit

→ gegenseitige Rücksichtnahme:

lange, nicht interaktive Prozesse → nice

[nice](#) : Prozess ressourcenschonend aufrufen

```
> nice bzip2 ganz_lange_datei
```

↪ was man normalerweise auch zum Starten eingibt



2. Block: Dateiverwaltung

Dateien verwalten

- vieles kennen wir schon: pwd, ls, cd, cp, mv, rm, ...

Weitere typische Werkzeuge

- Lese-/Schreibrechte verwalten
- Dateien nach Namen finden
- Komprimieren und archivieren



Lese- und Schreibrechte

3-stufiges System von Berechtigungen

Besitzer (ihr!) Gruppe Alle (Vorsicht!)

```
> ls -li
-rw-rw-r--  cg stud 1973 2005-09-06 11:56 dax.csv
-rw-r----- cg stud 8457 2005-09-05 11:37 leer.sxi
drwxr-xr-x  cg stud  48 2005-09-06 11:57 verzeichnis
```

Diagramm zur Berechtigungsstruktur:

- Ein blauer Pfeil zeigt von 'ls' zu den ersten drei Zeichen der ersten Zeile.
- Ein grüner Pfeil zeigt von 'li' zu den letzten beiden Zeichen der ersten Zeile.
- Ein grüner Pfeil zeigt von 'stud' zu den ersten beiden Zeichen der ersten Zeile.
- Ein roter Pfeil zeigt von 'Alle (Vorsicht!)' zu den letzten drei Zeichen der ersten Zeile.

Grundlegende Berechtigungen

r	read	(Öffnen/Lesen erlaubt)
w	write	(Schreibzugriff erlaubt)
x	execute	(Programmausführung erlaubt)



Zu welchen Gruppen gehöre ich?

[id](#) : identity

```
> id
```

```
uid=22227 (cg) gid=12000 (stud) groups=...
```

→ Zusätzliche Gruppen nur durch Statuswechsel
(Hiwi, Diplomand werden, ...)



Berechtigungen ändern

[chmod](#) : change file mode

> `chmod g-w datei` → kein Schreibzugriff für Gruppe

> `chmod u+w datei` → Schreibzugriff für sich selbst

> `chmod go-rwx *.txt`

→ bei *.txt-Dateien rwx für Gruppe und Alle wegnehmen

- **u** : Berechtigungen für **Besitzer** (**user**; erster **rwX**-Block)
- **g** : Berechtigungen für **Gruppe** (**group**; zweiter **rwX**-Block)
- **o** : Berechtigungen für **Alle** (**other**; dritter **rwX**-Block)



Berechtigungen von Verzeichnissen

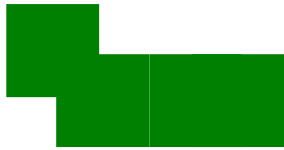
Anlegen und Löschen von Dateien:

→ Schreibberechtigung im aktuellen Unterverzeichnis

```
drwxr-xr-x cg users 352 2005-09-06 12:39 .
```

```
drwxr-xr-x cg users 2264 2005-09-06 14:05 ..
```

```
-rw-rw-r-- cg users 1973 2005-09-06 11:56 datei.csv
```

Berechtigungen von Verzeichnissen

In Verzeichnis wechseln / hineinsehen:

```
drwxr-xr-x  cg  users  96 2005-09-06 16:14 .  
drwxrwxrwt root root 1200 2005-09-06 16:00 ..  
drw-r--r-- cg  users  120 2005-09-06 14:20 ablage
```

```
> cd ablage
```

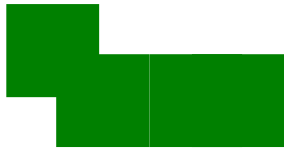
```
bash: cd: ablage: Permission denied
```

```
> chmod u+x ablage
```

```
> cd ablage
```

```
(erfolgreich)
```

→ Execute ('x')-Berechtigung für das Verzeichnis



Datei-Namen suchen

find : find files

Startverzeichnis, dessen Unterverzeichnisse mit durchsucht werden



```
> find . -name zwei.txt
./verzeichnis/zwei.txt
./zwei.txt
```

```
> find . -name "*.jpg"
./Fotos/img_1936.jpg
./Fotos/img_1939.jpg
usw.
```

sonst sucht die Shell im aktuellen Verzeichnis nach *.jpg und setzt deren Namen hier ein!



Freien Plattenspeicher feststellen

[df](#) : freien Plattenplatz anzeigen

```
> df -h .
```

Filesystem	1K-blocks	Used	Available	Use%	Mounted on
/dev/hda2	6.0G	1.8G	4.0G	32%	/

- Plattenplatz steht allen Benutzern zur Verfügung
→ bitte Rücksicht nehmen
- Administrator kann maximalen Verbrauch pro Benutzer begrenzen



Eigenen Plattenspeicherverbrauch

[du](#) : disc usage

```
> cd                               wechselt ins Home-Verzeichnis
> du -hs .                          mein gesamter Speicherverbrauch
198M .
```

```
> du -hs *                          Verbrauch im Unterverzeichnis
6.5M   Vorkurs-1
1.8M   Vorkurs-2
2.7M   Vorkurs-3
... weitere Dateien und Unterverzeichnisse ...
```



Einzelne Dateien komprimieren

Komprimieren von Dateien (verlustlos!):

- > `gzip datei.txt` → `datei.txt.gz`
- > `bzip2 datei.txt` → `datei.txt.bz2`
- > `xz datei.txt` → `datei.txt.xz`
- > `zip datei.zip datei.txt`

Entkomprimieren von Dateien:

- > `gunzip datei.txt.gz`
- > `bunzip2 datei.txt.bz2`
- > `unxz datei.txt.xz`
- > `unzip datei.zip`



Mehrere Dateien archivieren

[tar](#) : tape archiver

- > **tar cf ~/archiv.tar *.txt Fotos**
→ packt Dateien und Verzeichnisse in ein Archiv
- > **tar tvf archiv.tar**
→ zeigt Inhalt des Archivs
- > **tar xf archiv.tar**
→ alles wieder auspacken
- > **tar xf archiv.tar eins.txt**
→ nur die angegebenen Dateien wieder auspacken



Archive komprimieren

tar alleine komprimiert nicht

1. tar-Datei hinterher komprimieren

> **gzip archiv.tar**

→ erzeugt Datei archiv.tar.gz

2. und vor dem Auspacken wieder dekomprimieren

> **gunzip archiv.tar.gz**

→ erzeugt wieder archiv.tar



Automatisch (de-)komprimieren

tar kann gzip/bzip2 automatisch anwenden

z – Option um gzip zu verwenden

j – Option um bzip2 zu verwenden

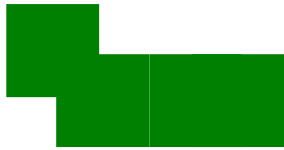
J – Option um xz zu verwenden

> **tar czf archiv.tar.gz *.txt ...**

→ Datei-Archiv erzeugen und komprimieren

> **tar xzf archiv.tar.gz**

→ Datei-Archiv entkomprimieren und auspacken



Dateityp erkennen

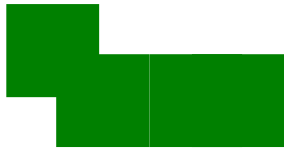
file : file type

```
> mv archiv.tar.gz archiv
```

```
> file archiv
```

```
archiv: gzip compressed data, was  
"archiv.tar", from Unix
```

→ nützlich wenn die Dateinamens-Erweiterung fehlt
oder unbekannt ist



3. Block: E-Mail

- E-Mail-Adressen und Header
- Die „Netiquette“ - angemessener Umgang mit E-Mail
- Historie, SMTP-Protokoll und dessen Schwächen
- Signaturen mit GPG erstellen und prüfen
- E-Mail-Programme



E-Mail-Adressen (1)

Beispiel: juser @ techfak.uni-bielefeld.de

local part

domain part

@ als Trennzeichen

local part ~ Benutzer / user

domain part ~ FQDN (fully qualified domain)



E-Mail-Adressen (2)

domain part unterscheidet nicht
zwischen Groß- und Kleinschreibung:

juser@techfak.uni-bielefeld.de

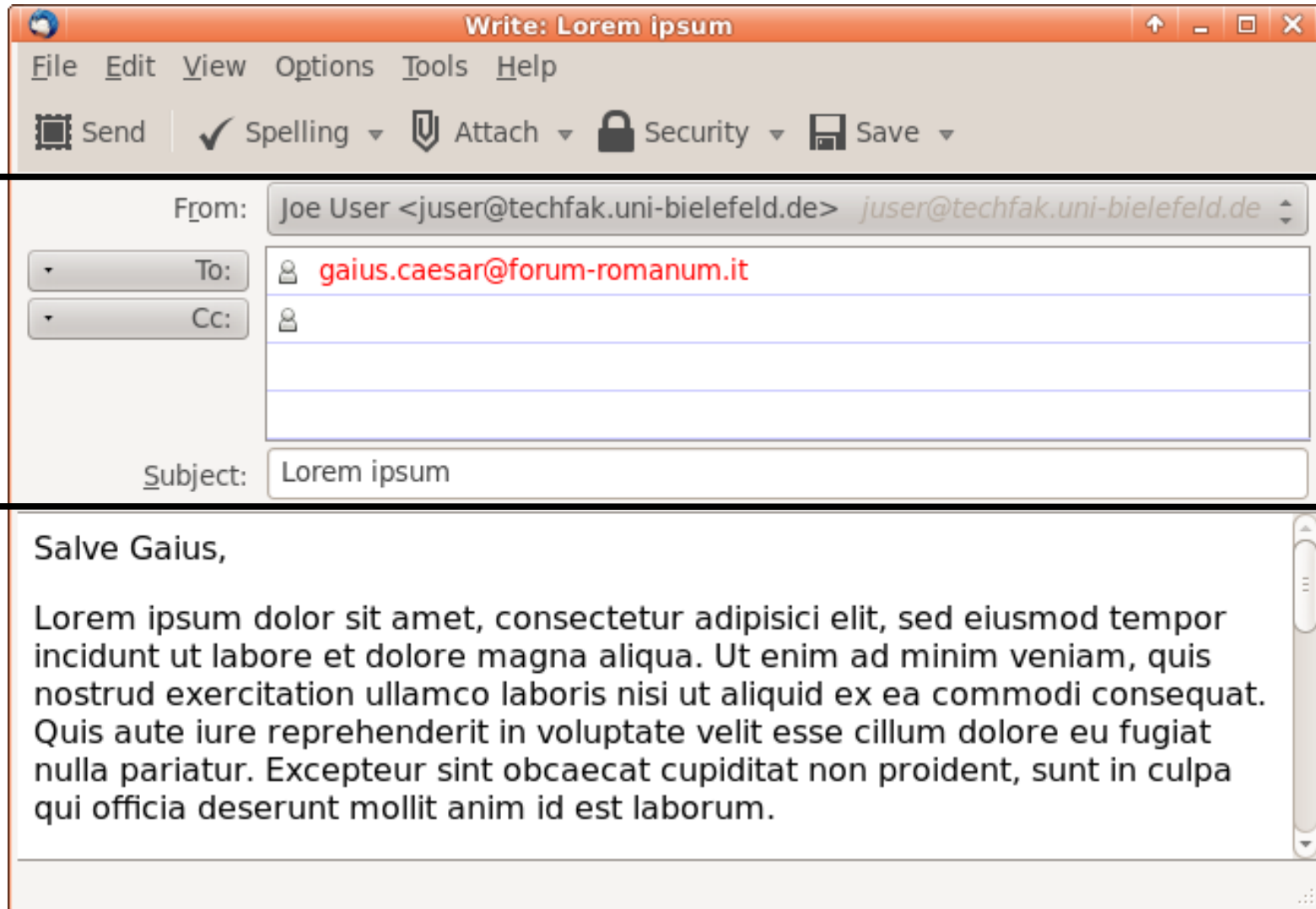
juser@TechFak.Uni-Bielefeld.DE

juser@tEchfak.unI-bieLEfeLD.dE

kommt alles beim gleichen Empfänger an!



Header und Body



Header

„Briefumschlag“

Body

„Briefpapier“



Header – typische Felder

From: Absender der E-Mail (ggf. voreingestellt)

To: Empfänger der E-Mail

Cc: indirekte Empfänger, nur zur Kenntnisnahme
(cc = carbon copy, Durchschlagpapier)

Bcc: wie Cc:, wird aber aus abgesandter Mail entfernt
(bcc = blind carbon copy)



Body

Inhalt:

- 7bit ASCII (erinnert euch an gestern)
- ansonsten frei, aber *Netiquette* sollte man einhalten

Netiquette = Benimmregeln im Netz, u.a. E-Mail



Anrede, Schlußformel (1)

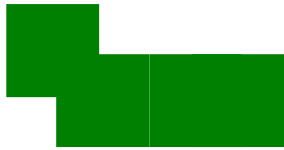
E-Mail ist ungezwungener als förmliche Korrespondenz

- es gibt leichte Präferenz zu “Du” anstelle von “Sie”
- „Sie“ kann distanzierend / abwertend interpretiert werden

Es gilt situationsbedingt zu unterscheiden - Gegenbsp:

- Behörden
- Kommunikation mit Vorgesetzten
- Bewerbungsschreiben
- offizielle Firmenschreiben

vorher fragen/
recherchieren!



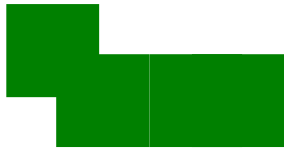
Anrede, Schlußformel (2)

„Sehr geehrter...“

„Mit freundlichen Grüßen“

→ kann analog zu „Sie“ negativ interpretiert werden;
„Ich will nicht mit Dir kommunizieren, muss aber...“

Ausnahmen natürlich wieder möglich!



Anrede, Schlußformel (3)

Im Uni-Bereich oft zu lesen:

Liebe(r) Frau/Herr Name,

hier passt beides!

ich wende mich an Sie/Dich,...

Viele Grüße

Vorname Name



Signaturen

- Nicht mehr als vier Zeilen
- Signatortrenner „--“ verwenden
(Strich Strich Leerzeichen)
- Bei Firmen- und Behördenmails gelten andere Regeln



Stilistische Aspekte

Selbstverständlich:

- korrekte Rechtschreibung, Grammatik, Zeichensetzung
- insbesondere keine Leerzeichen vor Satzzeichen!
- Emoticons :-)
westlich
- (^_^)
japanisch

Nicht:

- ALLES GROß SCHREIBEN
- man schreibt auch nicht alle sätze klein
- mehrere Ausrufezeichen sind albern!!!!!!!1 1 eins1 !!1 elf!

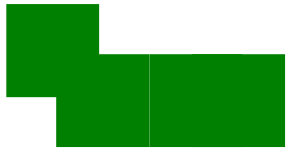


„TOFU“=Text oben, Full quote unten

```
Subject: Re: Lorem ipsum

Ist okay.
  Gaius

On 0002-09-18 20:25, Joe User wrote:
> Salve Gaius,
>
> Lorem ipsum dolor sit amet, consectetur adipiscing elit, sed eiusmod
> tempor incididunt ut labore et dolore magna aliqua. Ut enim ad minim
> veniam, quis nostrud exercitation ullamco laboris nisi ut aliquid ex
> ea commodi consequat. Quis aute iure reprehenderit in voluptate velit
> esse cillum dolore eu fugiat nulla pariatur. Excepteur sint obcaecat
> cupiditat non proident, sunt in culpa qui officia deserunt mollit
> anim id est laborum.
>
> Gruß
>   Joe User
>
> --
> Joe User - Max Mustermann der Informatik
> Technische Fakultät - Universität Bielefeld
>
>
>
```



Schlechtes Zitieren: „TOFU“ (2)

Weil es die Lesbarkeit des Textes verschlechtert.

> Warum ist TOFU so nervig?

>> TOFU

>>> Was ist das größte Ärgernis in Mails?



Besseres Zitieren (1)

> Wir planen ein Meeting mit dem
> Kunden zur besseren Abstimmung.
Gute Idee, das unterstütze ich!

Absatzweise zitieren
und antworten

> Ich schlage den 06.12. vor, um [...]
Da kann ich nicht wegen Nikolaus.

unwichtige Details
mit [...] kürzen

Viele Grüße

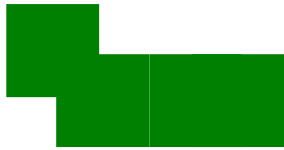
....



Besseres Zitieren (2)

Diskussion kann über mehrere Mailwechsel laufen:

- >> [Meeting mit dem Kunden] ← Kontext mit eigenen Worten zusammenfassen
 - >> Ich schlage den 06.12. vor, um [...]
 - > Da kann ich nicht wegen Nikolaus.
- Wie wäre es dann am 08.12.?



Aussagekräftige Subjects:

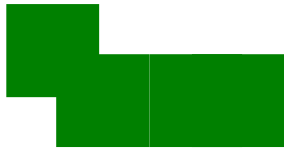
Subject: sollte vermitteln, *worum* es in der Mail geht

→ hilft dem Empfänger beim Sortieren, Priorisieren,
Wiederfinden

Schlechte Beispiele:

Subject: Frage

Subject: Hi!



Potentielle Spamwörter vermeiden

Subject: Hast Du die *Rechnung* schon bekommen?

Subject: Bring Deine *Frau* heute Abend zur Feier mit

Subject: Hast Du den Editor *vi* schon ausprobiert?

→ geht vielleicht automatisch in den Spamordner



Technische Aspekte (1)

HTML kann oder möchte nicht jeder lesen:

```
<!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Transitional//EN"
"http://www.w3.org/TR/xhtml1/DTD/xhtml1-transitional.dtd">
<html xmlns="http://www.w3.org/1999/xhtml" xml:lang="en" lang="en"><head>
<title></title>
<meta http-equiv="content-type" content="text/html; charset=utf-8"/>
<meta http-equiv="Content-Style-Type" content="text/css"/>
</head>
<body>
<div align="left"><font face="Arial" size="2"><span style="font-size:10pt">Liebe
Mitglieder des Rechnerausschusses,</span></font></div>
<div align="left"><font face="Arial" size="2"><span style="font-size:10pt"><br />
</span></font></div>
<div align="left"><font face="Arial" size="2"><span style="font-size:10pt">hier das
endg&#252;lt;tige Protokoll zur Sitzung vom Montag, 26.06.06.</span></font></div>
<div align="left"><font face="Arial" size="2"><span style="font-size:10pt">Es hat
keine Erg&#228;nzungen / &#196;nderungen zum Entwurf
gegeben.</span></font></div>
```



Technische Aspekte (2)

Gleiches gilt für Word (.doc) und andere Formate

am besten: reine **Text**mail

wenn graphische Formate unabdingbar sind:

- **PDF** als Anhang schicken
- in der Mail kurzer Hinweis darauf
- leere Mail mit .pdf-Anhang = Virusverdacht



Historie

E-Mail ist einer der ältesten Netzdienste

- Entwicklung war nicht geplant; es „ergab sich so“ weil Nutzer über das Netzwerk kommunizieren wollen
- 1982 RFC 822 „Urvater“ des E-Mail-Protokolls
- (RFC = „Request for Comments“
= Standards für Internetprotokolle)



E-Mail-Protokolle

Abholen/Lesen

- POP3 (veraltet), IMAP (Ports 143 und 993)

Absenden, Weiterleiten

- Simple Mail Transfer Protocol: SMTP
- textbasiertes Protokoll auf Port 25

→ textbasierte Protokolle kann man mit *telnet* "sprechen"



Nachteile von SMTP

- Keine Authentifizierung des Absenders!
- Zustellung kann beliebig lange dauern / E-Mail kann lautlos verloren gehen
- keine Empfangsbestätigung



Verschlüsselungstechniken

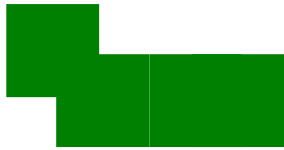
Verschlüsselung mit asymmetrischen Schlüsselpaaren

Unterzeichnen von E-Mails:

- Authentifizierung des Absenders;
E-Mail im Klartext für alle lesbar

Verschlüsseln von E-Mails:

- Authentifizierung des Absenders;
nur der Empfänger kann die E-Mail lesen



Kryptographische Unterschrift

juser@...

E-Mail
From: juser@...
To: mschaeff@...
Unterschrift: juser

unterschreiben

Geheimer
Schlüssel
juser@...

E-Mail versenden

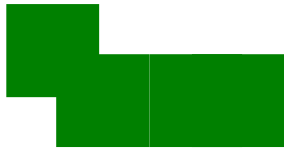
mschaeff@...

E-Mail
From: juser@...
To: mschaeff@...
Unterschrift: juser

prüfen

Öffentlicher
Schlüssel
juser@...

„Prüfen“ = Kommt die Mail vom Besitzer des geheimen Schlüssels?



Aufgaben für den Absender (juser)

- | | |
|--|--------------|
| 1. Schlüsselpaar generieren | |
| 2. Schlüssel mit E-Mail-Identität verbinden
(= E-Mail-Programm konfigurieren) | einmal |
| 3. Öffentlichen Schlüssel hochladen | |
| 4. Unterschriebene E-Mails versenden | beliebig oft |



Schlüsselpaar erzeugen

gpg : GNU Privacy Guard

juser erzeugt sich ein Schlüsselpaar:

> **gpg --gen-key**

[Voreinstellungen annehmen;
Name und E-Mail-Adresse wie im E-Mail-Profil
angeben]



Schlüssel mit E-Mail-Identität verbinden

Account Settings

Local Folders

- Junk Settings
- Disk Space
- ▼ juser@techfak.uni-bielefeld.de
 - Server Settings
 - Copies & Folders
 - Composition & Addressing
 - Junk Settings
 - Synchronization & Storage
 - OpenPGP Security**
 - Return Receipts
 - Security
 - Outgoing Server (SMTP)

OpenPGP Options (Enigmail)

Support for OpenPGP encryption and signing messages is provided by Enigmail. You need to have GnuPG (gpg) installed in order to use this feature.

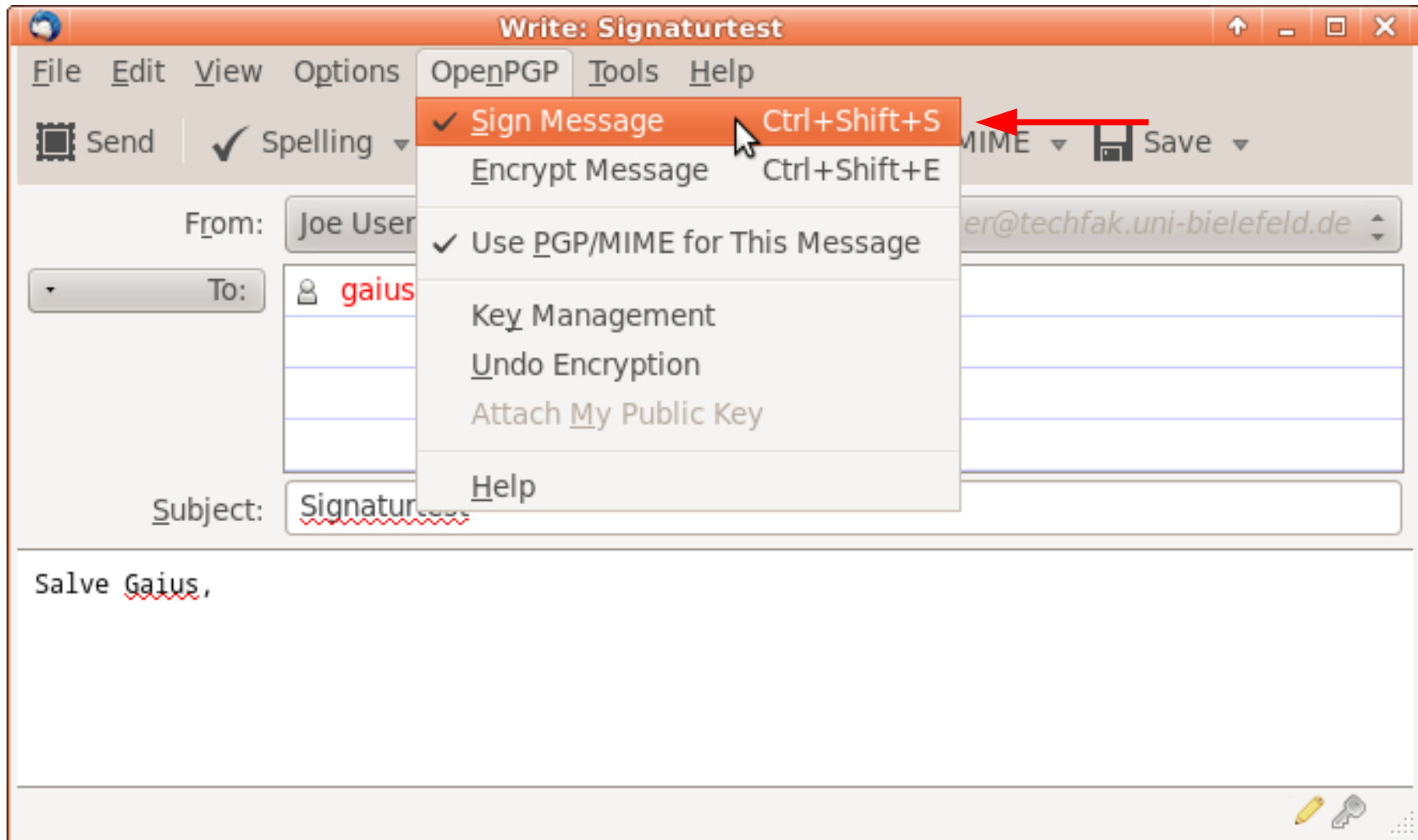
- Enable OpenPGP support (Enigmail) for this identity
 - Use email address of this identity to identify OpenPGP key
 - Use specific OpenPGP key ID (0x1234ABCD):

Message Composition Default Options

- Sign non-encrypted messages by default
- Sign encrypted messages by default
- Encrypt messages by default
- Use PGP/MIME by default



Unterschiedbene E-Mail versenden





Öffentlichen Schlüssel bereitstellen

juser „exportiert“ seinen öffentlichen Schlüssel:

```
> gpg --armor --export juser@techfak.uni-bielefeld.de
```

und lädt ihn auf seinen Webserver, etc.



Aufgaben für den Empfänger (mschaeff)

1. Öffentlichen Schlüssel von juser einholen
2. Fingerabdruck des Schlüssels prüfen
(Gehört der Schlüssel wirklich juser?)
3. Unterschriebene E-Mail öffnen

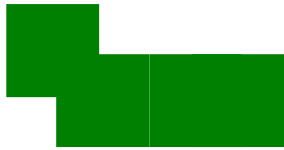


Öffentlichen Schlüssel einholen

1. Datei `joes_key.txt` herunterladen

2. Joes Schlüssel aufnehmen:

```
> gpg --import joes_key.txt
```

Vorsicht: Ist das wirklich Joes Schlüssel?

+ OpenPGP UNTRUSTED Good signature from Joe User <juser@techfak.uni-bielefeld.de> Details ▾

From Joe User ★

Subject **Signierte Mail**

To Mattias Schäffersmann ★

Reply Forward Archive Junk Delete

20:58

Other Actions ▾

Hallo Mattias,

hier ist eine signierte Mail.

Gruß
Joe





Folgendes Szenario (Original-Mail):

juser@...

E-Mail
Mein Konto ist
010020030

Unterschrift: juser

Geheimer
Schlüssel
juser@...

unterschreiben

E-Mail versenden

mschaeff@...

E-Mail
Mein Konto ist
010020030

Unterschrift: juser

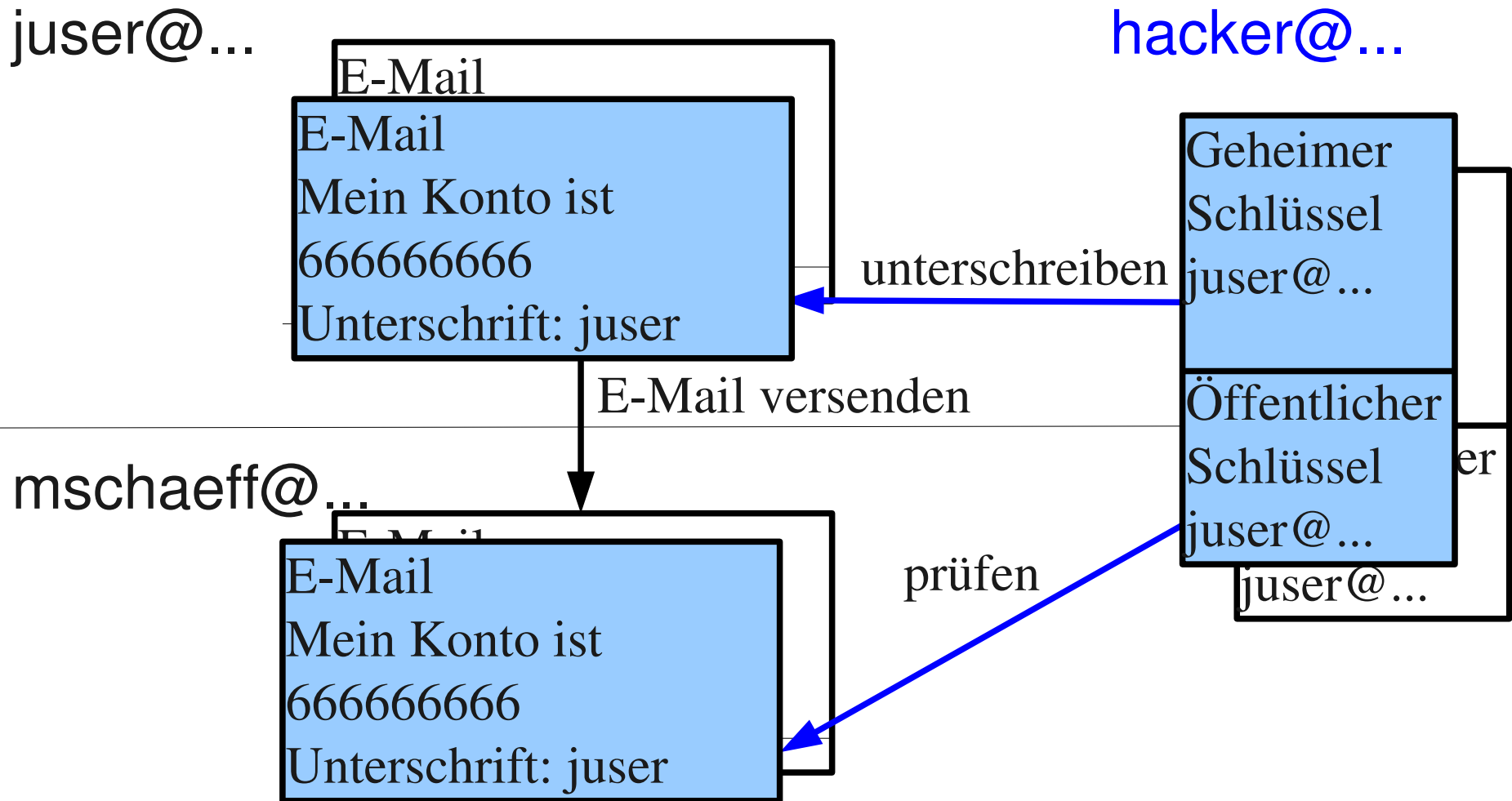
Öffentlicher
Schlüssel
juser@...

prüfen

„Prüfen“ = Kommt die Mail vom Besitzer des geheimen Schlüssels?



Folgendes Szenario (Gehackte-Mail):



„Prüfen“ = Kommt die Mail vom Besitzer des geheimen Schlüssels?



Überprüfen des Fingerabdruckes (1)

Jeder Schlüssel hat einen eindeutigen,
nicht fälschbaren Fingerabdruck:

```
> gpg --fingerprint juser@techfak.uni-bielefeld.de
pub 2048R/EB9220E0 2012-09-18
Key fingerprint = 925D 3C2E 208A 0257 F4BB 5487 8821 3FC8 EB92 20E0
uid Joe User <juser@techfak.uni-bielefeld.de>
sub 2048R/492B4EE0 2012-09-18
```



Überprüfen des Fingerabdruckes (2)

Fingerabdruck von Joe persönlich bestätigen lassen

- am Telefon vorlesen lassen
- von persönlich erhaltener Visitenkarte ablesen
- an ganz vielen Stellen im Netz nachlesen



Überprüfen des Fingerabdruckes (3)

Überprüften Schlüssel als gültig markieren:

(Voraussetzung: Empfänger (mschaeff) hat auch Schlüsselpaar)

```
> gpg --sign-key juser@techfak.uni-bielefeld.de
```



Unterschiedene E-Mail öffnen

+ OpenPGP Good signature from Joe User <juser@techfak.uni-bielefeld.de> Details ▾

From Joe User

Subject **Signierte Mail**

To Mattias Schäffersmann

Reply Forward Archive Junk Delete

20:58

Other Actions ▾

Hallo Mattias,

hier ist eine signierte Mail.

Gruß
Joe



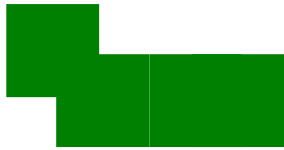


Verschlüsselung ist sehr komplexes Thema

zum weiteren Einlesen:
Wikipedia, Stichwort gpg

was man auch wissen sollte:

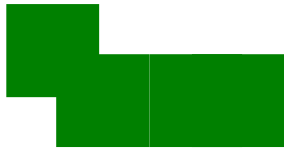
- Funktionsweise des „Web of Trust“
- komplettes Verschlüsseln von E-Mails



Bei uns vorhandene E-Mail-Clients

unter anderem:

- Thunderbird (empfohlener Client)
- Evolution (Gnome)
- Kontact / Kmail (KDE)
- mutt (Kommandozeile)



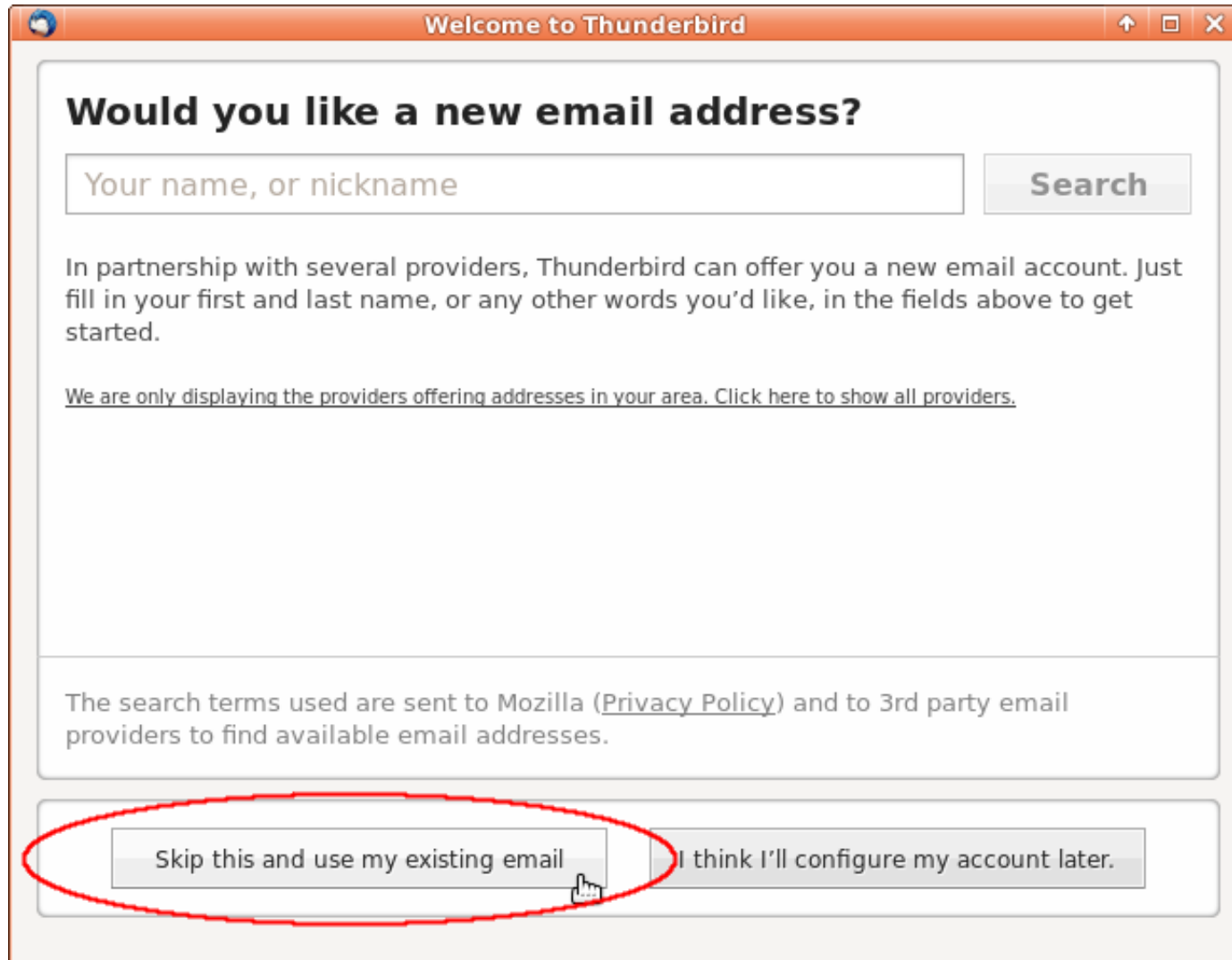
Beispielkonfiguration Thunderbird

> **thunderbird**

Danach erscheinen die folgenden Dialoge:



Beispielkonfiguration Thunderbird (1)





Beispielkonfiguration Thunderbird (2)

Mail Account Setup

Your name: Your name, as shown to others

Email address:

Password:

Remember password



Beispielkonfiguration Thunderbird (3)

Mail Account Setup

Your name: Your name, as shown to others

Email address:

Password:

Remember password

Looking up configuration: Trying common server names 🌀



Beispielkonfiguration Thunderbird (4)

The screenshot shows the 'Mail Account Setup' dialog box with the following configuration:

- Your name: Joe User
- Email address: juser@techfak.uni-bielefeld
- Password: [Redacted]
- Remember password:
- Incoming: IMAP, Server hostname: imap.techfak.uni-bielefeld.de, Port: 143, SSL: STARTTLS, Authentication: Autodetect
- Outgoing: SMTP, Server hostname: smarthost.techfak.uni-bie, Port: 25, SSL: STARTTLS, Authentication: Autodetect
- Username: juser

Buttons at the bottom: Get a new account, Advanced config, Cancel, **Re-test** (circled in red), Done.



Beispielkonfiguration Thunderbird (5)

Mail Account Setup

Your name: Your name, as shown to others

Email address:

Password:

Remember password

The following settings were found by probing the given server

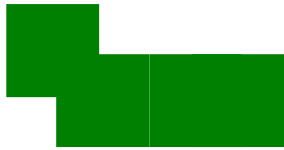
	Server hostname	Port	SSL	Authentication
Incoming:	IMAP <input type="text" value="imap.techfak.uni-bielefeld.de"/>	143 <input type="text"/>	STARTTLS <input type="text"/>	Normal password <input type="text"/>
Outgoing:	SMTP <input type="text" value="smarthost.techfak.uni-bielefeld.de"/>	25 <input type="text"/>	STARTTLS <input type="text"/>	Normal password <input type="text"/>

Username:

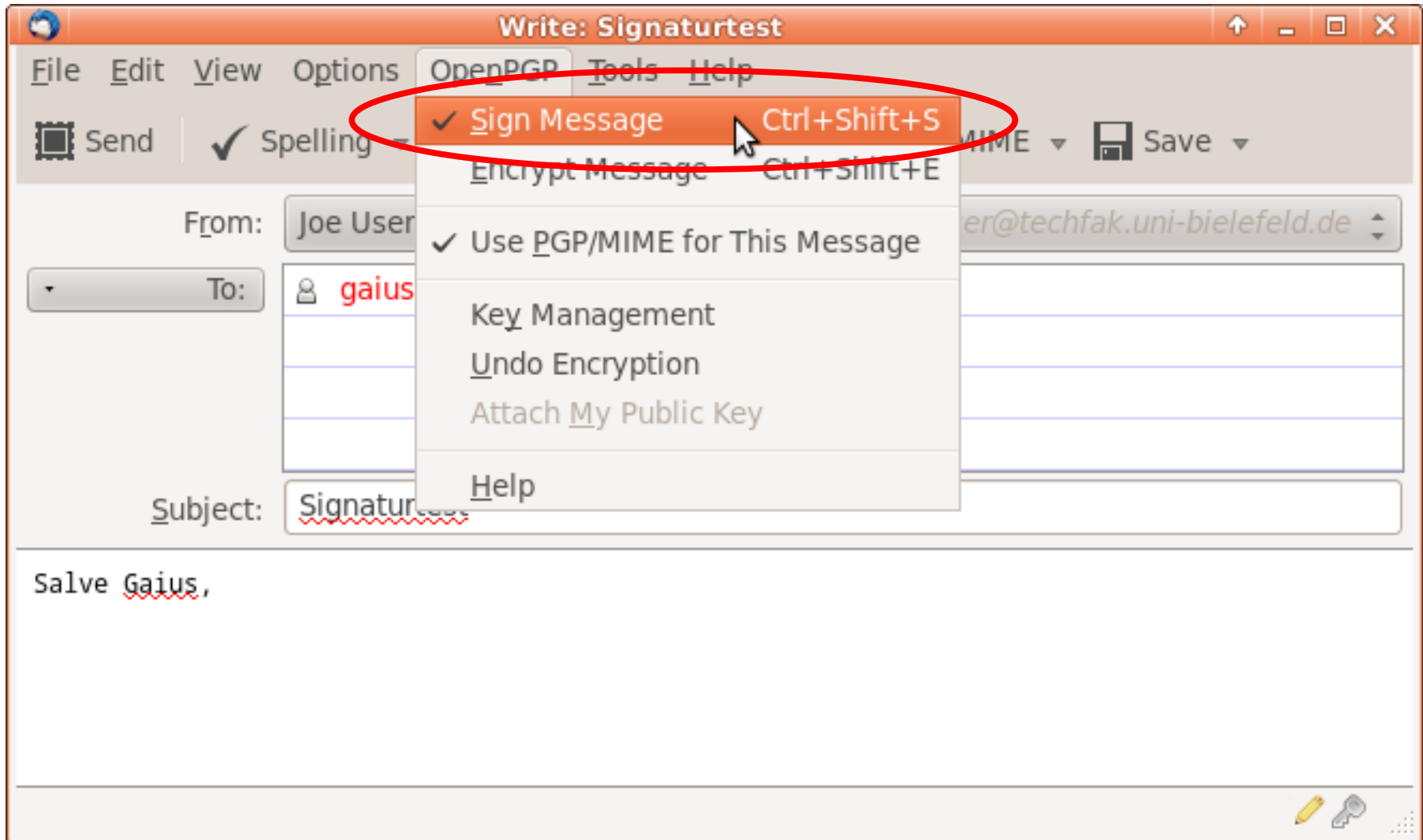


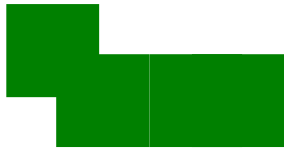
Enigmail für GPG installieren

- Im Menüpunkt „Tools“ „Add-ons“ auswählen
- Nach „enigmail“ suchen
- Enigmail 1.4.4 (oder neuer) installieren
- Thunderbird neu starten
- Im Menüpunkt „Edit“ „Account Settings“ auswählen
- Links „OpenPGP Security“ auswählen
- Rechts „Enable OpenPGP support [...]“ auswählen
- Beide „Sign (non-)encrypted messages by default“ aktivieren
- „Use PGP/MIME by default“ aktivieren



Unterschriebene E-Mail senden





Ende des heutigen Vortrags

Danke fürs Zuhören!

Bis morgen