

BESTIMME, WER DEINE MAILS KENNT!

EIN CRYPTO-WORKSHOP



binarybugs | presented by SDS Jena | 11.12.2018

[binarybugs\(at\)riseup.net](mailto:binarybugs(at)riseup.net) | binarybugs.org | [@binarybugs](https://twitter.com/binarybugs)

Überblick

// Ein paar einleitende Worte

// Neuland aka Internet

// E-Mails & Crypto-Basics

// How-to Verschlüsseln

// Ran an die Rechner!

// Abschluss



Das Ziel des Workshops

// verstehen, warum E-Mail Verschlüsselung super ist

// verschlüsselte E-Mails verschicken und erhalten

// mehr Lust auf Crypto!



<< Seid großartig zueinander und tut Dinge! >>



// Für Anfänger*innen

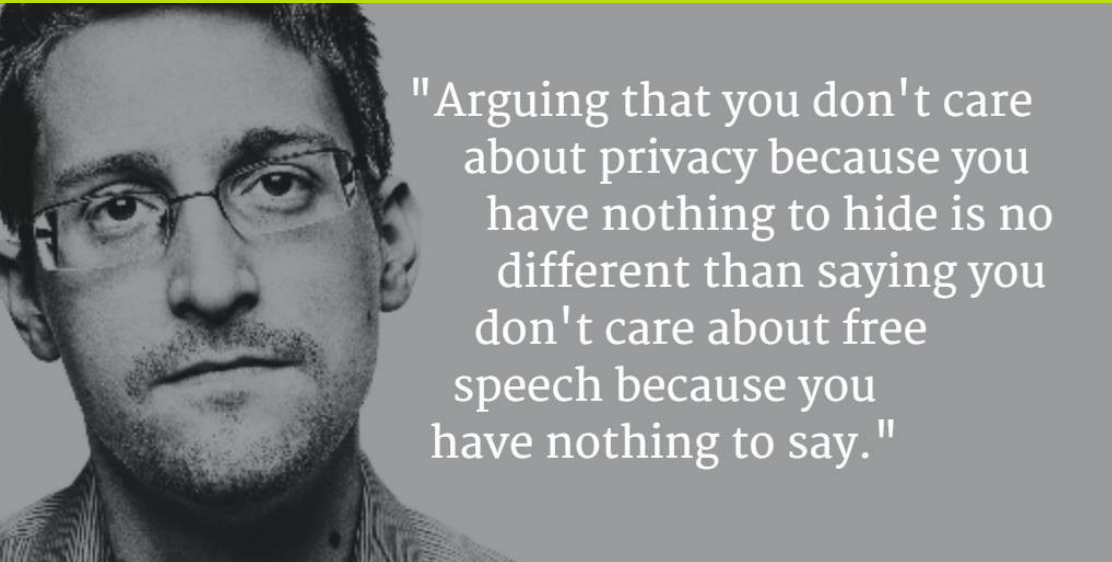
// Verständlichkeit

// Fragt!

// Probiert's aus!



**<< Ich habe nichts zu verbergen,
denn ich tue ja nichts verbotenes >>**

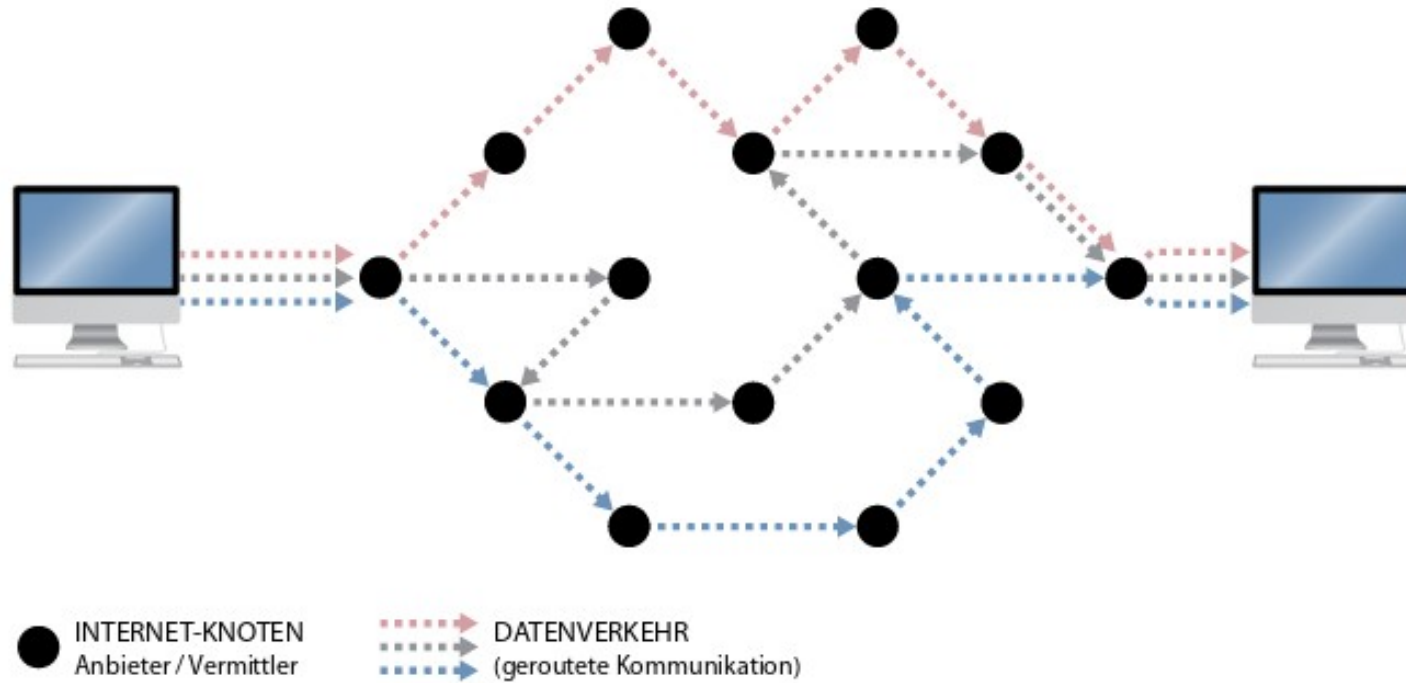


Netzpolitik.org: CC BY-NC-SA 4.0

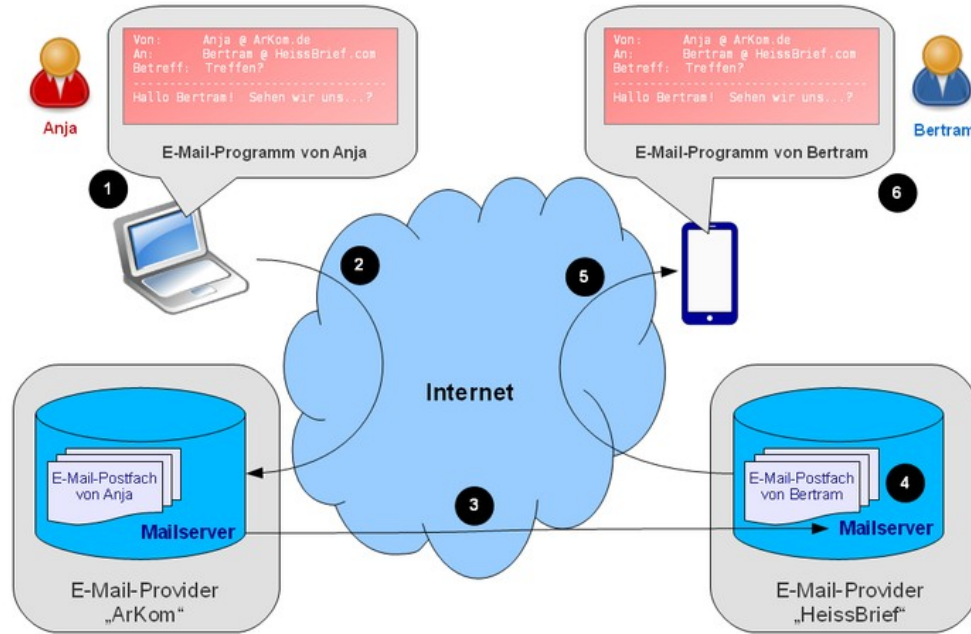
Allgemeine Erklärung der Menschenrechte, Art. 12



Ein Netzwerk aus Computernetzwerken



Der Weg einer E-Mail



IM WORKSHOP:



verschlüsselte Kommunikationswege **nicht** anonyme



HTTPS_TLS/SSL

1. Schritt:



Johann H. : CC BY-SA 3.0

Mein PC



verschlüsselt



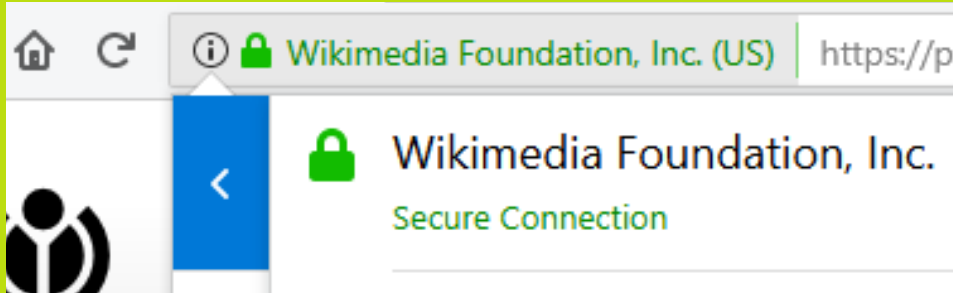
Johann H. : CC BY-SA 3.0

Server

[anderer Rechner, der
irgendwo steht]



HTTPS_TLS/SSL



Mozilla : CC BY-SA 3.0



E-Mails: Fragen, die sich stellen

2. Schritt:

// Warum ist es wichtig, welchen Webmailanbieter ich nutze?

// Welche sind zu empfehlen?

// Warum noch zusätzlich E-Mails verschlüsseln?

// Wie?



Webmailanbieter

KOSTENFREI?

// IN DER REGEL ZAHLEN WIR MIT UNSEREN DATEN \\\

<< Google has most of my email because it has all of yours>> (B. M. Hill)

Protonmail (kostenfrei)

Posteo.de (1€ pro Monat)

Mailbox.org (1€ pro Monat)

Riseup.net (kostenfrei)

...



Wer meine E-Mails mitlesen kann

// Absender*in, Empfänger*in

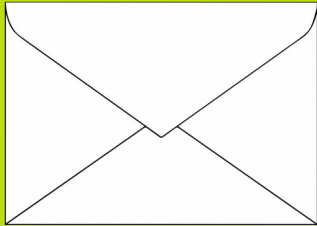
// Mailanbieter (web.de, gmx, gmail...) von Absender*in u.
Empfänger*in

// Menschen, die Datenkreuzungen im Internet kontrollieren
(meist irgendwelche großen Firmen)

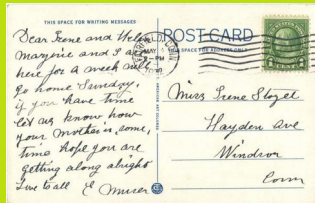
// Noch mehr, wenn mensch sich Mühe gibt



E-Mail Verschlüsselung



VS.



// Soll niemensch verstehen können (Vertraulichkeit)

// Manipulationen erkennen (Integrität)

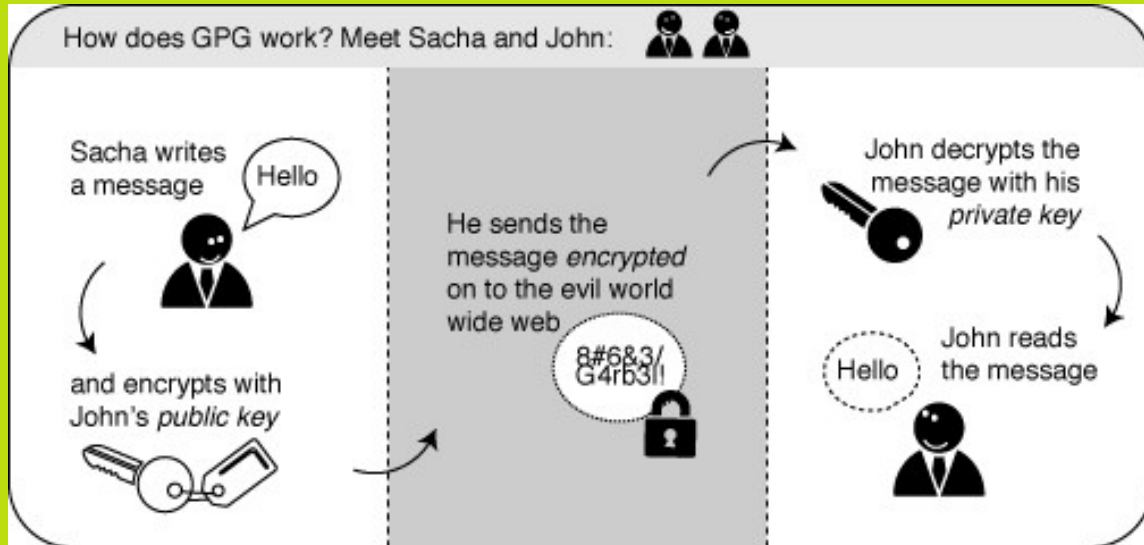
...wurde die Nachricht manipuliert?

...wurde der*die Absender*in manipuliert?

: verschlüsseln und signieren



Crypto-Basics: Verschlüsseln



CC BY-SA 3.0

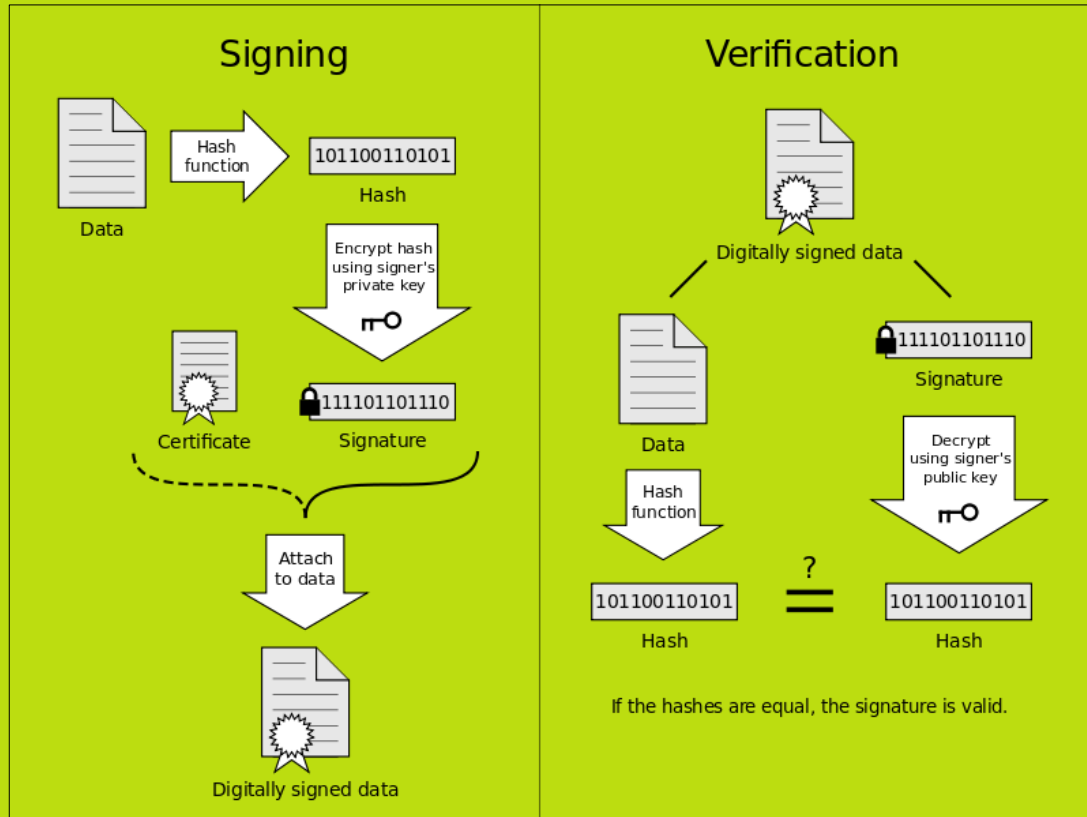
// privater und öffentlicher Schlüssel

// privat ist privat!

// öffentlicher Schlüssel ist jeder*m bekannt



Crypto-Basics: Signieren





// Hash der Nachricht wird mit meinem privaten Schlüssel verschlüsselt




[meine Nachricht wird durch eine Funktion geschoben und es kommt eine kurze Zeichenkette raus]



Crypto-Basics: Verschlüsseln

Datei Bearbeiten Ansicht Optionen Enigmail Extras Hilfe

 Senden  Rechtschr. ▾  Anhang ▾  S/MIME ▾  Speichern

Enigmail:    Meinen öffentlichen Schlüssel anhängen

Von: cane <cane@privacy-handbuch.de>

An: Beatrice <beatrice@server.tld>

An:

Betreff: Verschlüsselte E-Mail

Hallo,

Privacy Handbuch : CC BY-SA 3.0

// Verschlüsseln & signieren



Los geht's:



// Installation von
mozilla thunderbird
GnuPG



// Add-on Enigmail



The image shows a web browser window displaying the Thunderbird website. The browser's address bar shows the URL `https://www.thunderbird.net/de/`. The website features the Thunderbird logo, navigation links for THUNDERBIRD, ADD-ONS, HILFE, and SPENDEN, and a large heading: "Software für den einfachen Umgang mit E-Mails." Below this, a paragraph states: "Thunderbird ist eine freie E-Mail-Anwendung, die man einfach einrichten und anpassen kann — und sie ist voll mit tollen Funktionen!" A prominent green button labeled "Kostenloser Download" is centered on the page. At the bottom of the website, there are links for "Systeme & Sprachen", "Was ist neu", and "Datenschutz".

Overlaid on the bottom of the website is a preview of the Thunderbird application interface. The interface includes a sidebar with folders like "Posteingang", "Entwürfe", "Gesendet", and "Papierkorb". The main pane shows an email from "alex.thunder@example.com" with a subject line "Betreff". The top of the application window has tabs for "Posteingang", "Kalender", "Aufgaben", and "Chat". A search bar and a "Schnellfilter" (quick filter) are also visible. On the right side of the application window, there is a "Termine" (calendar) panel showing the date "22 Sa" and "Aug 2015 KW 34".

The Windows taskbar at the bottom of the screen shows the search bar with the text "Suchbegriff hier eingeben", several application icons, and the system clock displaying "15:36" and "09.12.2018".



// How-to Verschlüsseln

The screenshot shows the Thunderbird email client interface. The main window displays the 'Konten' (Accounts) section with options to 'Konto einrichten' (Set up account) for E-Mail, Chat, and New. Below this, there's a section for 'Einen neuen Kalender erstellen' (Create a new calendar).

Overlaid on the Thunderbird window is a dialog box titled 'Konto für eine bestehende E-Mail-Adresse einrichten' (Set up account for an existing email address). The dialog contains the following fields and options:

- Ihr Name:** Vorname Nachname (Your name, as others see it)
- E-Mail-Adresse:** ich@example.com (Existing email address)
- Passwort:** Passwort (Password)
- ☒ **Passwort speichern** (Save password)

Below these fields, it states: 'Einstellungen wurden bei Ihrem Anbieter des E-Mail-Diensts gefunden' (Settings found at your email provider). It offers two options: ☒ **IMAP** (Nachrichten auf dem Server speichern) and ☐ **POP3** (Nachrichten auf diesem Computer speichern).

Server settings listed:

- Posteingangs-Server: IMAP, imap.uni-jena.de, SSL
- Postausgangs-Server: SMTP, smtp.uni-jena.de, STARTTLS
- Benutzername: aileen.mirasyedi@uni-jena.de

Buttons at the bottom: 'Neue E-Mail-Adresse erhalten...' (Get new email address...), 'Manuell bearbeiten' (Manually edit), 'Fertig' (Done), and 'Abbrechen' (Cancel).

In the background, a PayPal donation page is visible, showing a 'Spenden per PayPal' button and a '10 €' amount. The page also includes a 'SICHER' (Secure) lock icon and text about data processing.

At the bottom of the Thunderbird window, a status bar message reads: 'Durch die Integration der Erweiterung Lightning enthält Thunderbird nun Kalenderfunktionen.' (Due to the integration of the Lightning extension, Thunderbird now contains calendar functions.)





The screenshot shows the GnuPG Download page in Mozilla Firefox. The browser's address bar displays the URL <https://gnupg.org/download/index.html>. The page features the GnuPG logo with a "20 years" anniversary banner. A navigation menu includes links for Home, Donate, Software, Download, Documentation, and Blog. The "DOWNLOAD" section contains a note about downloading the GNU Privacy Guard from a mirror site and a "Donate" button. The "SOURCE CODE RELEASES" section explains the canonical release forms of GnuPG and provides a table of packages.

DOWNLOAD

Note that you may also download the GNU Privacy Guard from a mirror site close to you. See our [list of mirrors](#). The table below provides links to the location of the files on the primary server only.

[Donate](#)

SOURCE CODE RELEASES

These are the canonical release forms of GnuPG. To use them you need to build the binary version from the provided source code. For Unix systems this is the standard way of installing software. For GNU/Linux distributions are commonly used (e.g. Debian, Fedora, RedHat, or Ubuntu) which may already come with a directly installable packages. However, these version may be older so that building from the source is often also a good choice. Some knowledge on how to compile and install software is required.

The table lists the different GnuPG packages, followed by required libraries, required tools, optional software, and legacy versions of GnuPG. For end-of-life dates see further down.

Name	Version	Date	Size	Tarball	Signature
GnuPG	2.2.11	2018-11-06	6406k	download	download



The screenshot shows the Thunderbird Add-ons website interface. At the top, there's a navigation bar with 'Posteingang', 'Add-ons-Verwaltung', and 'Enigmail :: Suche :: Add-ons'. A search bar contains 'Enigmail'. A blue banner at the top says 'Willkommen bei den Thunderbird-Add-ons. Fügen Sie Zusatzfunktionen und Stile hinzu, um sich Thunderbird zu Eigen zu machen.' Below this, a 'Software-Installation' dialog box is open, displaying a warning: 'Sie sollten Add-ons nur von Quellen installieren, denen Sie vertrauen.' It lists the selected add-on as 'Enigmail' with its URL. The background shows search results for 'Enigmail' and 'Mail Redirect'.

Neu registrieren oder anmelden | Andere Anwendungen

Add-ons

ERWEITERUNGEN THEMES SAMMLUNGEN MEHR...

Suche Enigmail

Willkommen bei den Thunderbird-Add-ons. Fügen Sie Zusatzfunktionen und Stile hinzu, um sich Thunderbird zu Eigen zu machen.

Filterergebnisse

KATEGORIE
Alle Add-ons

FUNKTIONIERT MIT
Alle Versionen von Thunderbird
Alle Systeme

SCHLAGWORT
Alle Schlagwörter

93 passende Ergebnisse

Suchergebnisse

Sortieren nach

Enigmail
Versteck deine E-Mails mit Verschlüsselung und PGP-Schlüsseln.
★★★★★ (41) · 9.041 Benutzer

Mail Redirect
Erlaubt das Umleiten von E-Mails zu anderen Empfängern.
★★★★★ (128) · 36.526 Benutzer

Software-Installation

Sie sollten Add-ons nur von Quellen installieren, denen Sie vertrauen.

Bösartige Software kann Dateien auf Ihrem Computer beschädigen oder Ihre Privatsphäre verletzen.

Sie haben folgendes Add-on zur Installation ausgewählt:

Enigmail
<https://addons.thunderbird.net/thunderbird/downloads/latest/enigmail/addon-71-la>

Jetzt installieren Abbrechen

hinzufügen

hinzufügen

Zu Thunderbird hinzufügen

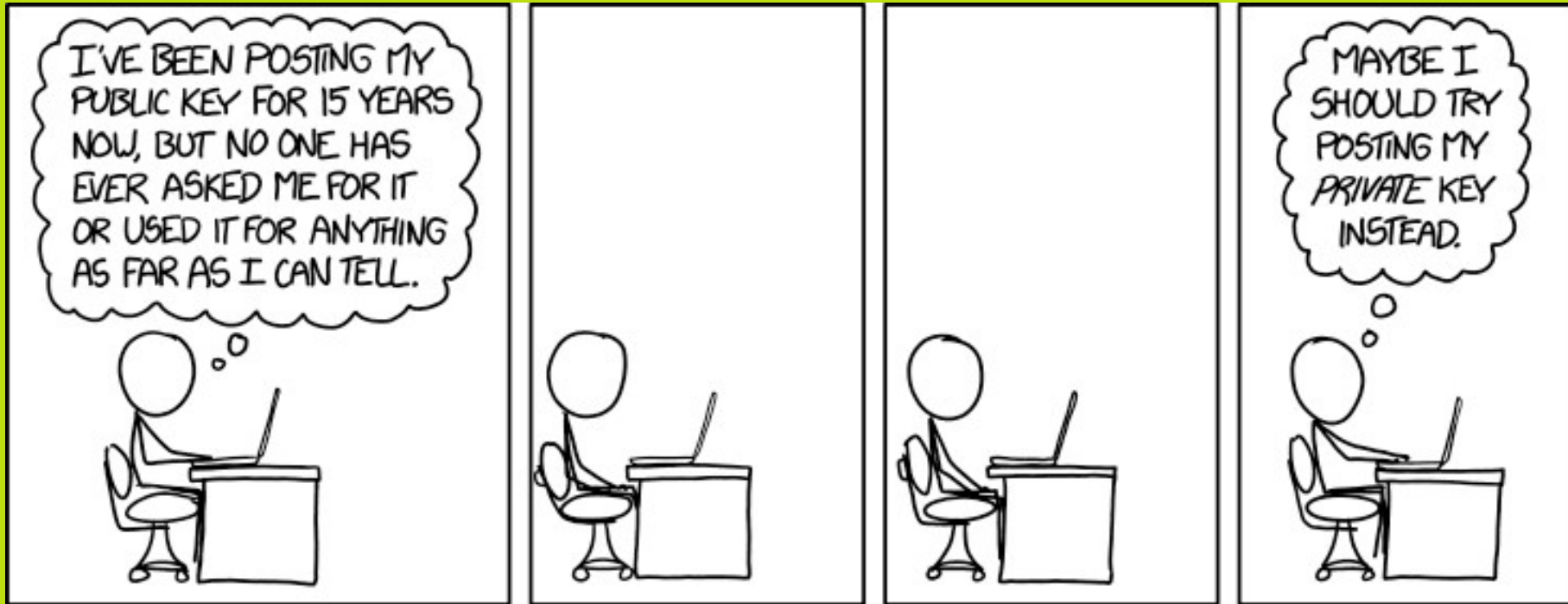
Zu Thunderbird hinzufügen

Suchbegriff hier eingeben

15:49 09.12.2018



Und jetzt?

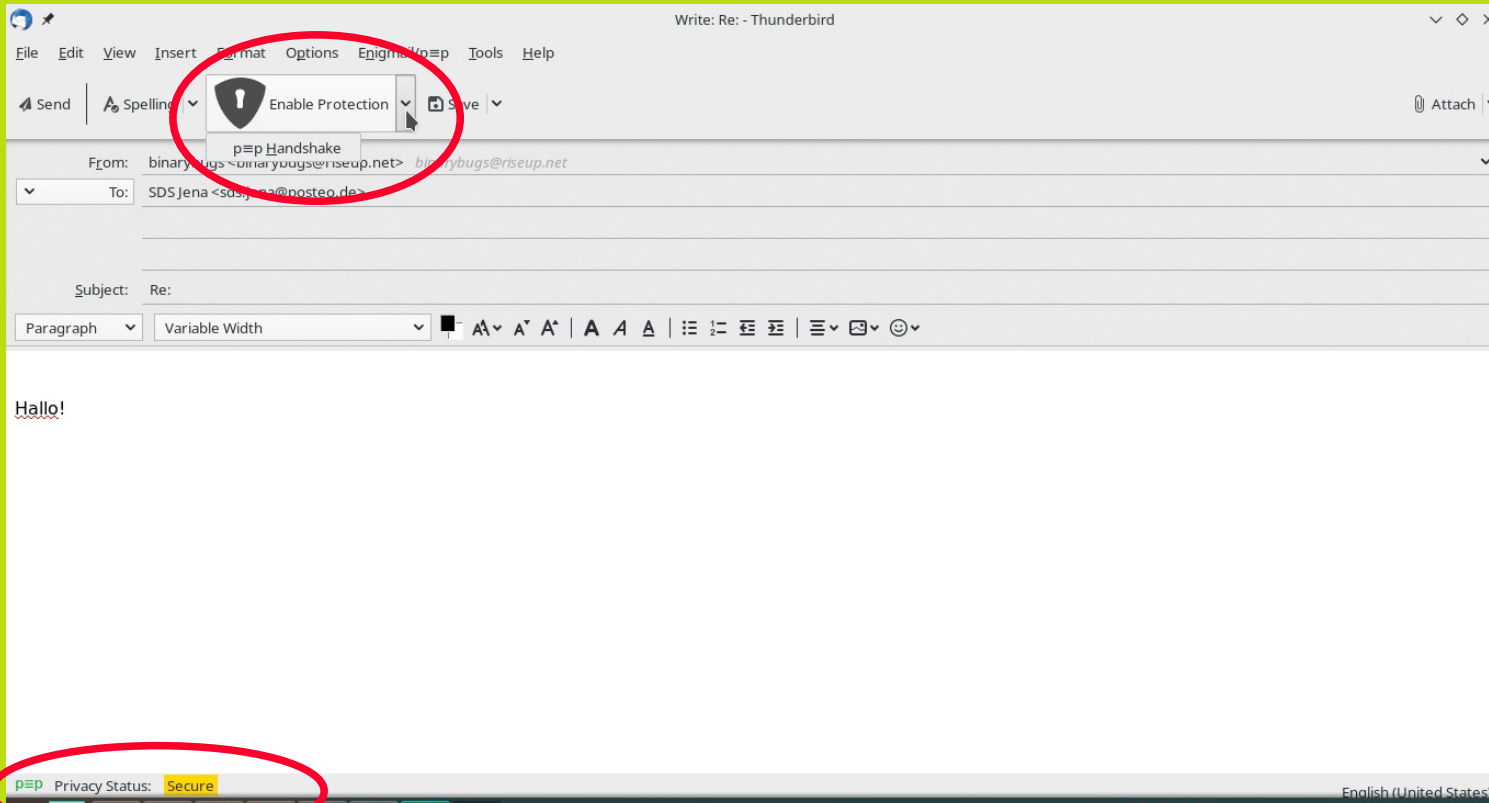


xkcd : CC BY-NC 2.5



// How-to Verschlüsseln

p=p



p≡p



Ran an die Rechner!



Don't forget the handshake ;)

// Oder auch so:



Ein paar abschließende Gedanken

// Sicherungskopie des privaten Schlüssels

// Sperrzertifikat

// Verschlüsselung für unterwegs

// Verschlüsselung der eigenen (gespeicherten) Daten

// Verschlüsselte E-Mail Kommunikation ist keine Einbahnstraße

// und auch kein Allheilmittel

// informiert bleiben!



Zum Nachschauen und Weiterlesen:

// www.cryptoparty.in

// www.privacy-handbuch.de

// https://digitalegesellschaft.de/wp-content/uploads/2012/04/digiges_wie_das_internet_funktioniert.pdf

// <https://myshadow.org/resources#Videos>

// <https://www.pep.security/index.html.de>



Danke für eure Aufmerksamkeit!

