

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

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

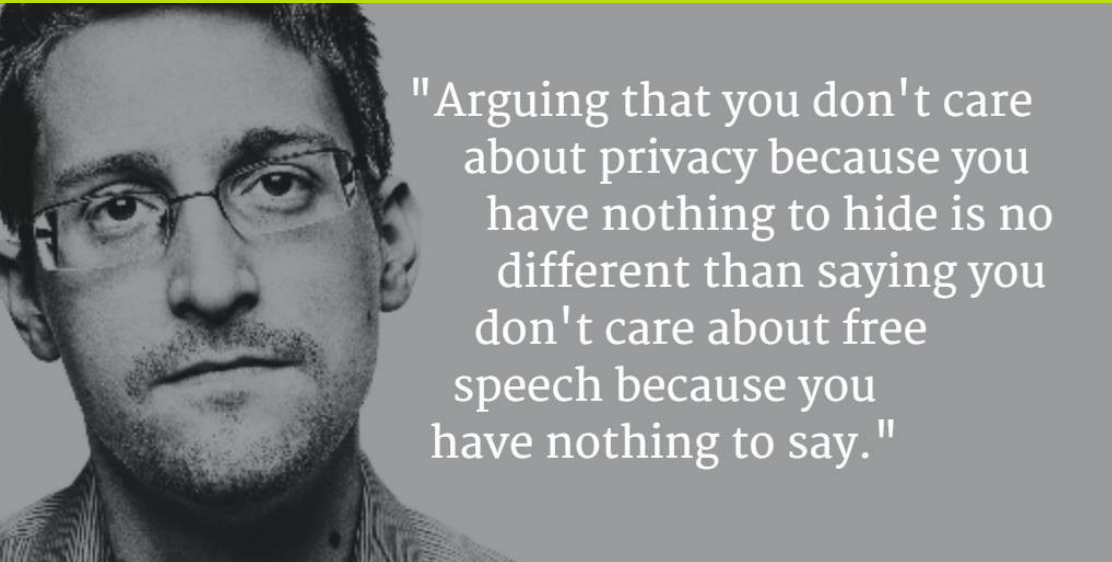
// Verständlichkeit

// Fragt!

// Probiert's aus!



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

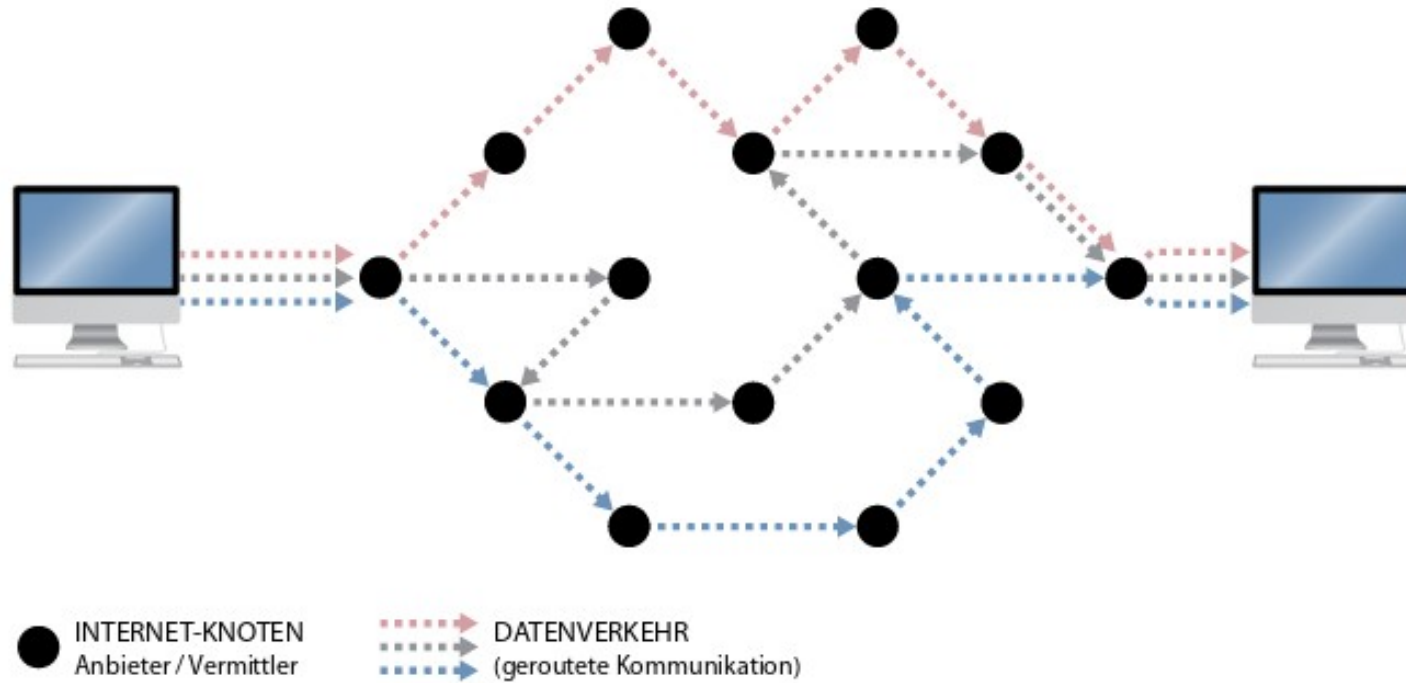


Netzpolitik.org: CC BY-NC-SA 4.0

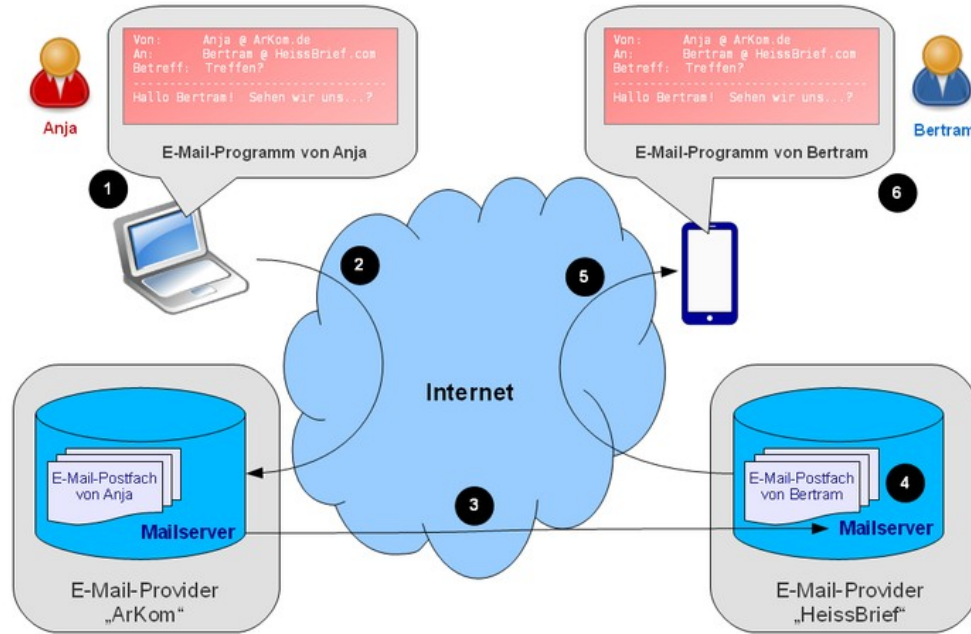
Allgemeine Erklärung der Menschenrechte, Art. 12



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



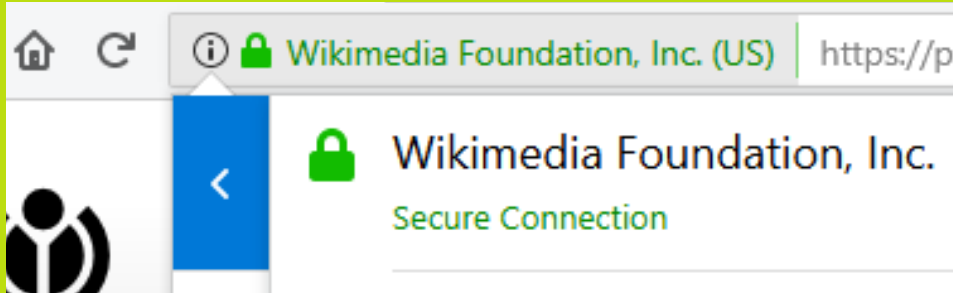
Johann H. : CC BY-SA 3.0

Server

[anderer PC, der irgendwo steht]



HTTPS_TLS/SSL



Mozilla : CC BY-SA 3.0

// wird bei der Mail Client

Konfiguration noch wichtig sein...



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

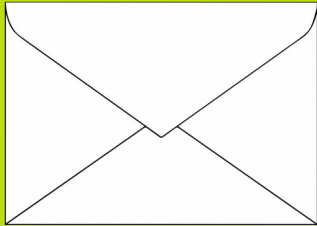
// Mailanbieter (web.de, gmx, gmail...) von Absender*in u.
Empfänger*in

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

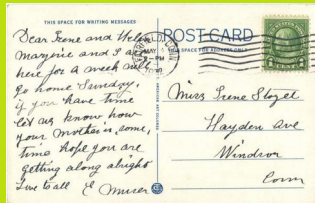
// Noch mehr, wenn mensch sich Mühe gibt



E-Mail Verschlüsselung



VS.



// Soll niemensch verstehen können (Vertraulichkeit)

// Manipulationen erkennen (Integrität)

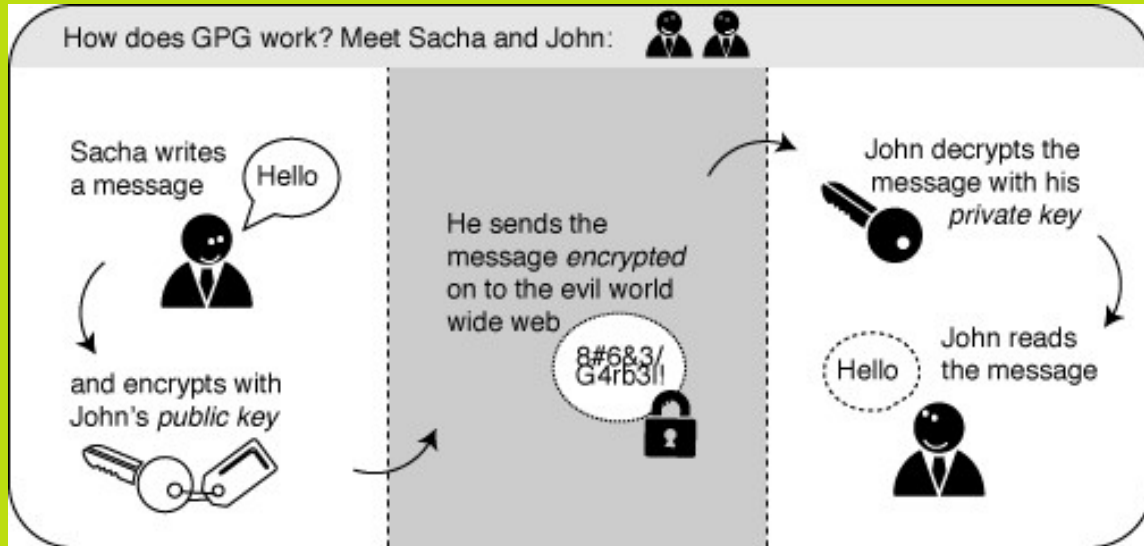
...wurde die Nachricht manipuliert?

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

: verschlüsseln und signieren



Crypto-Basics: Verschlüsseln



CC BY-SA 3.0

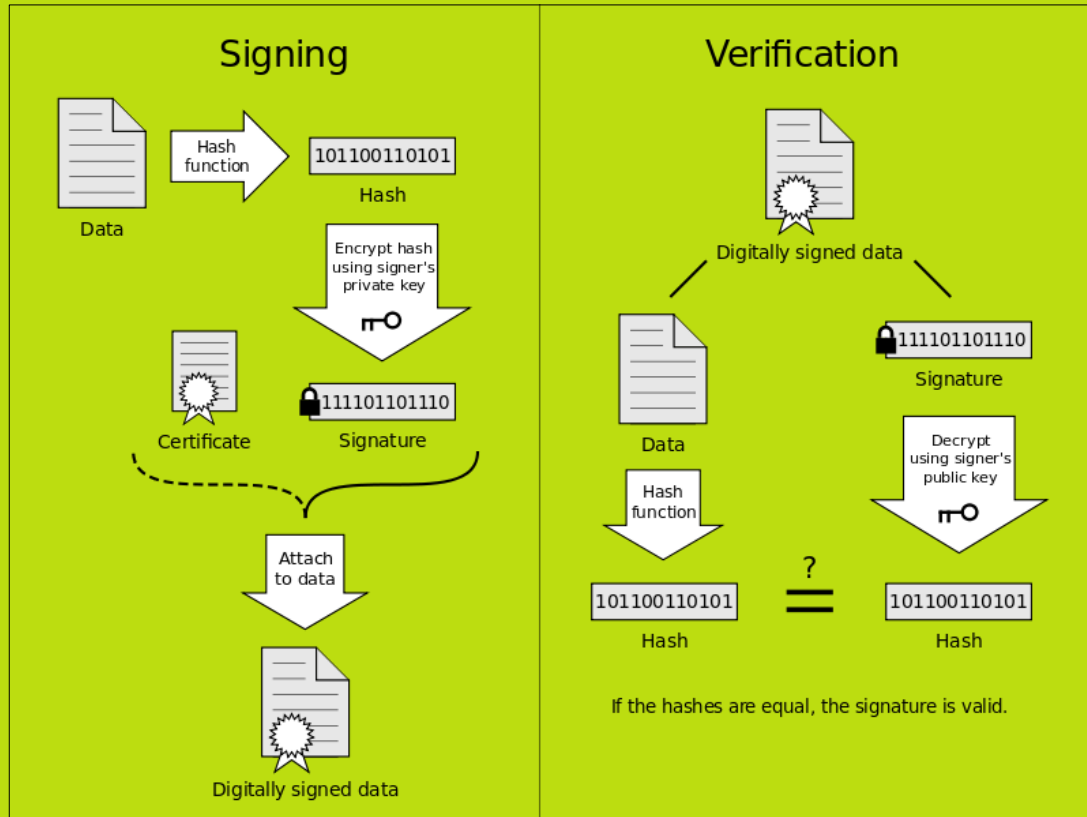
// privater und öffentlicher Schlüssel

// 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 email client 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 interface 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 interface, there is a "Termine" (calendar) view showing the date "22 Sa" (Saturday, August 22, 2015) and a "Neuer Termin" (New Event) button.

The Windows taskbar at the bottom of the screen shows the search bar with the text "Suchbegriff hier eingeben" and several application icons, including the Start button, File Explorer, and the Thunderbird icon. The system clock in the bottom right corner displays the time "15:36" and the date "09.12.2018".



// How-to Verschlüsseln

The screenshot displays the Thunderbird email client interface. The main window shows the 'Konten' (Accounts) section with options to 'Konto einrichten' (Set up account) and 'Einen neuen Kalender erstellen' (Create new calendar). A dialog box titled 'Konto für eine bestehende E-Mail-Adresse einrichten' (Set up account for an existing email address) is open, showing fields for 'Ihr Name' (Your name), 'E-Mail-Adresse' (Email address), and 'Passwort' (Password). The 'Passwort speichern' (Save password) checkbox is checked. Below these fields, the settings for the email account are displayed, including the IMAP and POP3 options, the incoming and outgoing mail servers, and the username.

In the background, a PayPal donation page is visible, showing a 'Spenden per PayPal' (Donate via PayPal) button and a 'Zu übermittelnde Daten festlegen' (Specify data to be transmitted) button. The page also displays a '10 €' donation amount and a 'SICHER' (Secure) status.

At the bottom of the Thunderbird window, a status bar indicates: '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 tabs for 'Posteingang', 'Add-ons-Verwaltung', and 'Enigmail :: Suche :: Add-ons'. The main header features the 'Add-ons' logo and a search bar containing 'Enigmail'. A blue banner below the header reads: 'Willkommen bei den Thunderbird-Add-ons. Fügen Sie Zusatzfunktionen und Stile hinzu, um sich Thunderbird zu Eigen zu machen.' On the left, there are filter options under 'Filterergebnisse' including 'KATEGORIE', 'FUNKTIONIERT MIT', and 'SCHLAGWORT'. The main content area shows search results for 'Enigmail', with a 'Suchergebnis' section. A 'Software-Installation' dialog box is prominently displayed in the center, warning the user: 'Sie sollten Add-ons nur von Quellen installieren, denen Sie vertrauen.' It lists the selected add-on as 'Enigmail' with its URL. At the bottom of the dialog are buttons for 'Jetzt installieren' and 'Abbrechen'. The background shows details for the 'Enigmail' add-on, including its description, ratings, and a 'Zu Thunderbird hinzufügen' button. The Windows taskbar at the bottom shows the search bar and several application icons. The system tray on the right indicates the date and time as 15:49 on 09.12.2018.

Neu registrieren oder anmelden | Andere Anwendungen

Termine < > X

9 So < > X
Dez 2018 KW 49

Neuer Termin

Heute

Morgen

Demnächst (5 Tage)

Filterergebnisse

KATEGORIE >>

Alle Add-ons

FUNKTIONIERT MIT >>

Alle Versionen von Thunderbird

Alle Systeme

SCHLAGWORT >>

Alle Schlagwörter

93 passende Ergebnisse

Suchergebnis

Sortieren nach

Enigmail

Verfügen

Op

★

Ma

Ma

★

Ed

Benötigt Neustart

This module allows you to change/edit email subjects

★★★★★ (41) · 9.041 Benutzer

Mail Redirect

Benötigt Neustart VORGESTELLT

Erlaubt das Umleiten von E-Mails zu anderen Empfängern

★★★★★ (128) · 36.526 Benutzer

Jetzt installieren Abbrechen

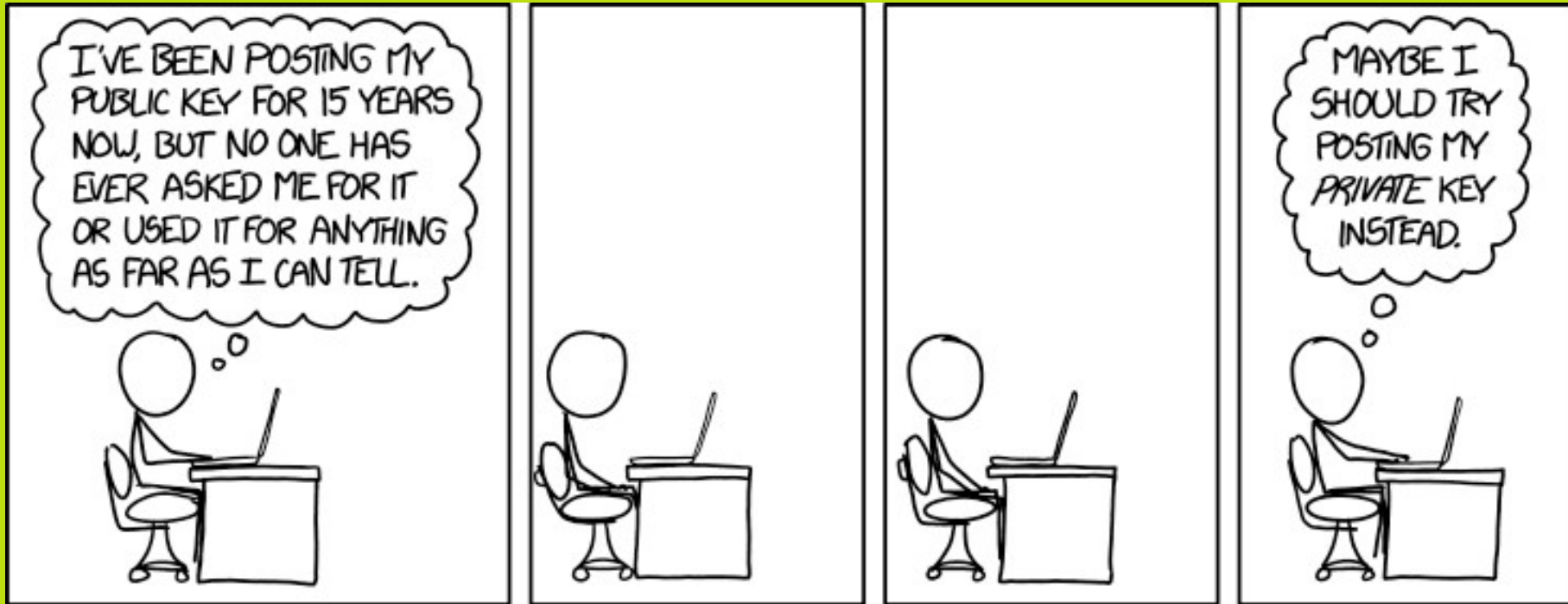
Zu Thunderbird hinzufügen

Suchbegriff hier eingeben

15:49
09.12.2018



Und jetzt?

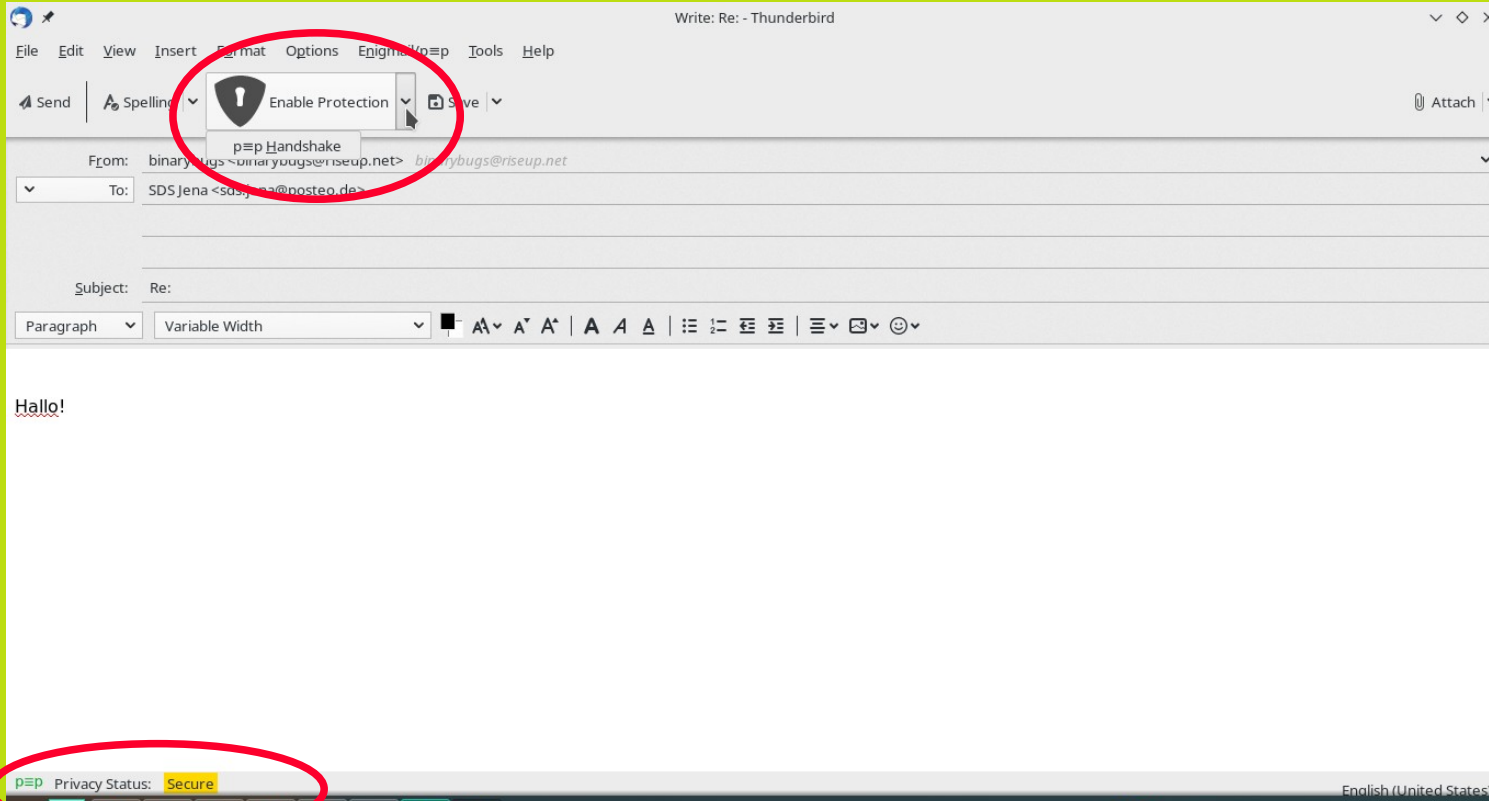


xkcd : CC BY-NC 2.5



// 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

//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!

