

# 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](http://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

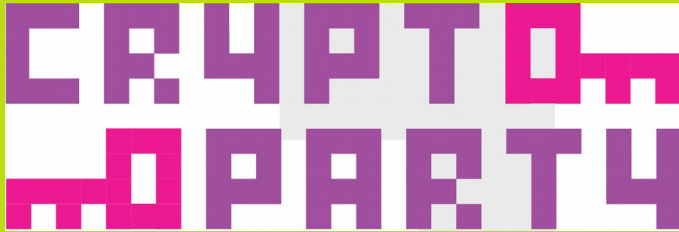
// verstehen, warum E-Mail Verschlüsselung super ist

// verschlüsselte E-Mails verschicken und erhalten

// mehr Lust auf Crypto!



**<< Seid großartig zueinander und tut Dinge! >>**



// Für Anfänger\*innen

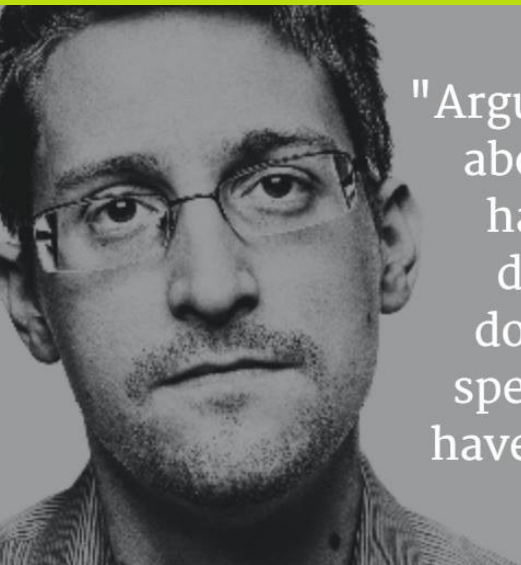
// Verständlichkeit

// Fragt!

// Probiert's aus!



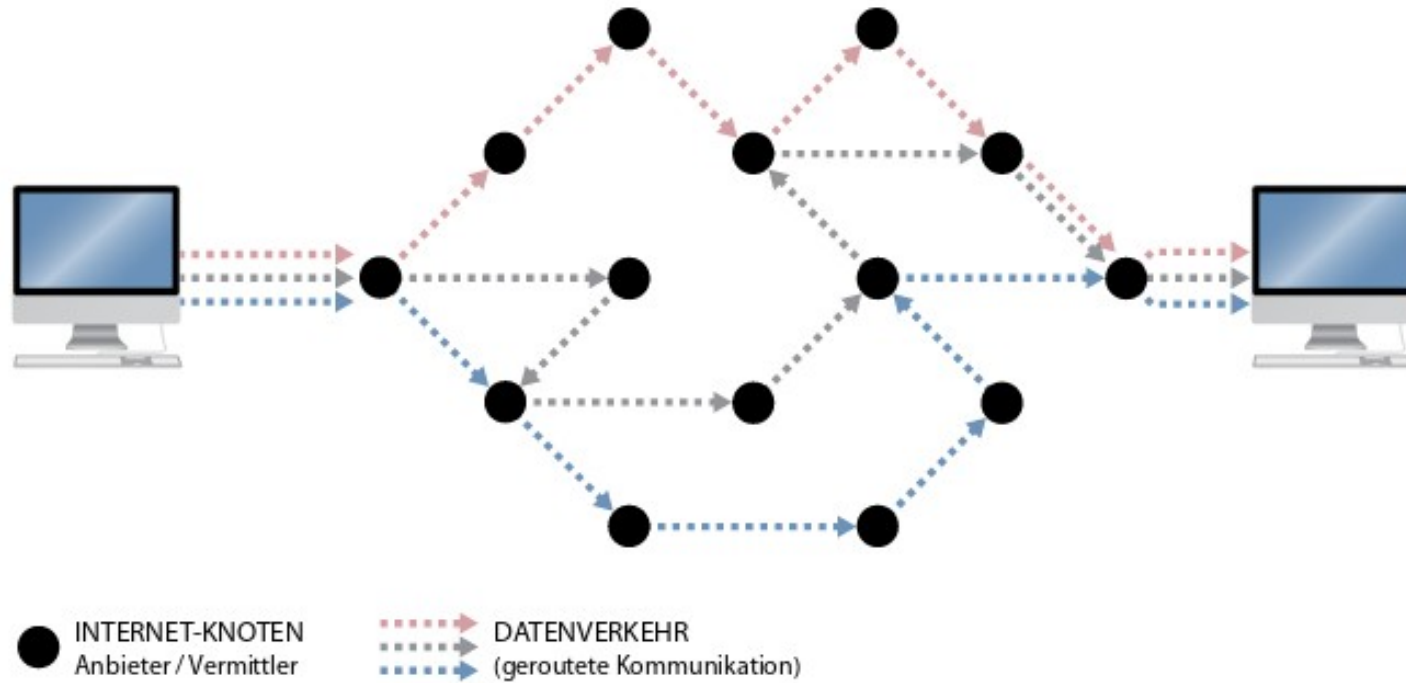
**<< Ich habe nichts zu verbergen,  
denn ich tue ja nichts verbotenes >>**



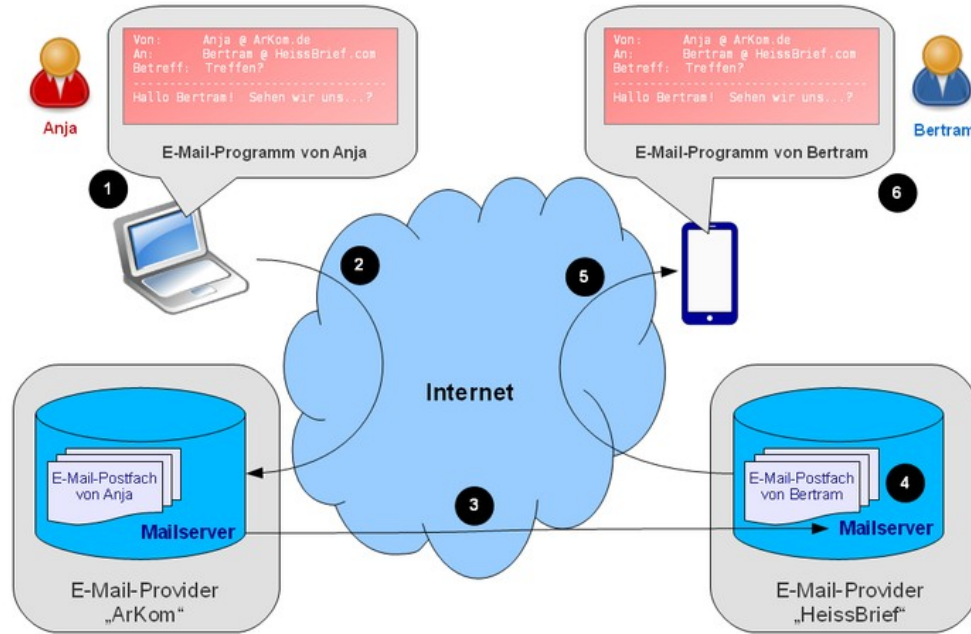
"Arguing that you don't care about privacy because you have nothing to hide is no different than saying you don't care about free speech because you have nothing to say."



# 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



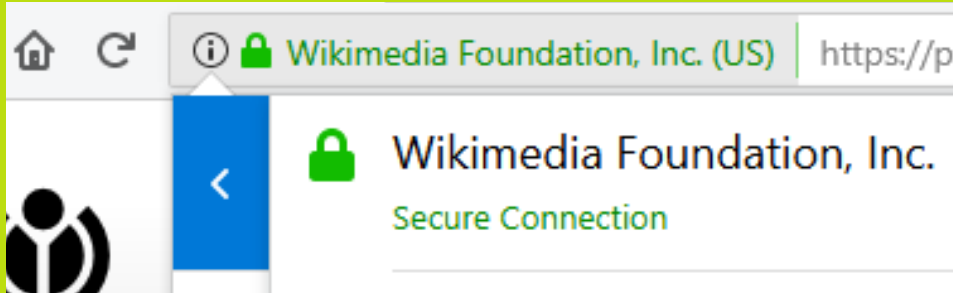
Johann H. : CC BY-SA 3.0

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

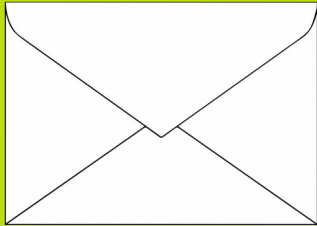
// Mailanbieter (web.de, gmx, gmail...) von Absender\*in u.  
Empfänger\*in

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

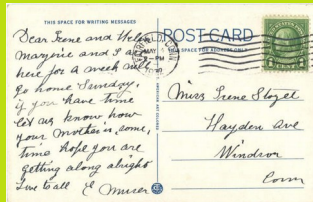
// Noch mehr, wenn mensch sich Mühe gibt



# E-Mail Verschlüsselung



VS.



// Soll niemensch verstehen können (Vertraulichkeit)

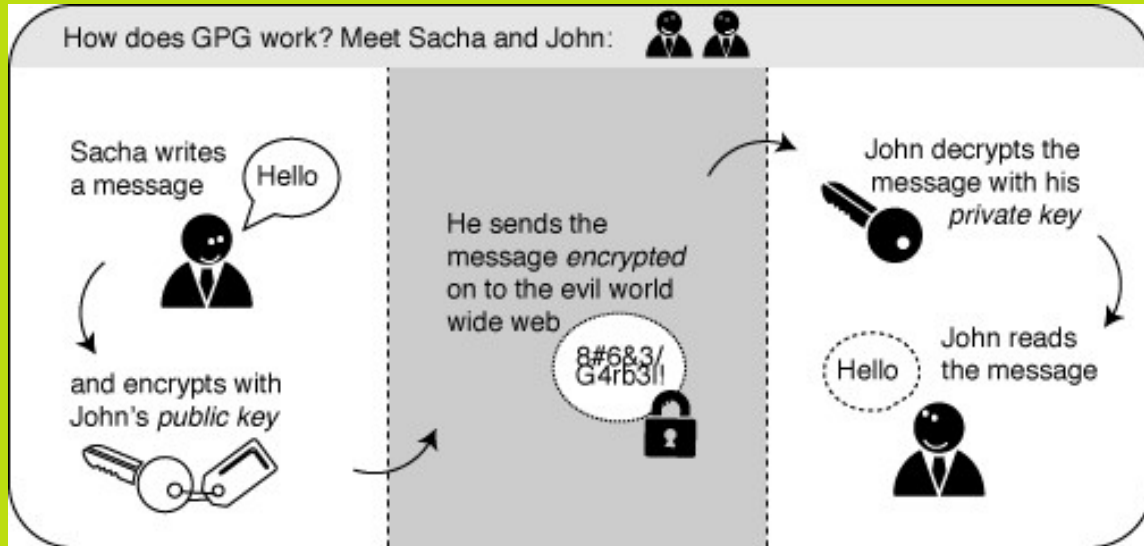
// Manipulationen erkennen (Integrität)

...wurde die Nachricht manipuliert?

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



# Crypto-Basics: Verschlüsseln



CC BY-SA 3.0

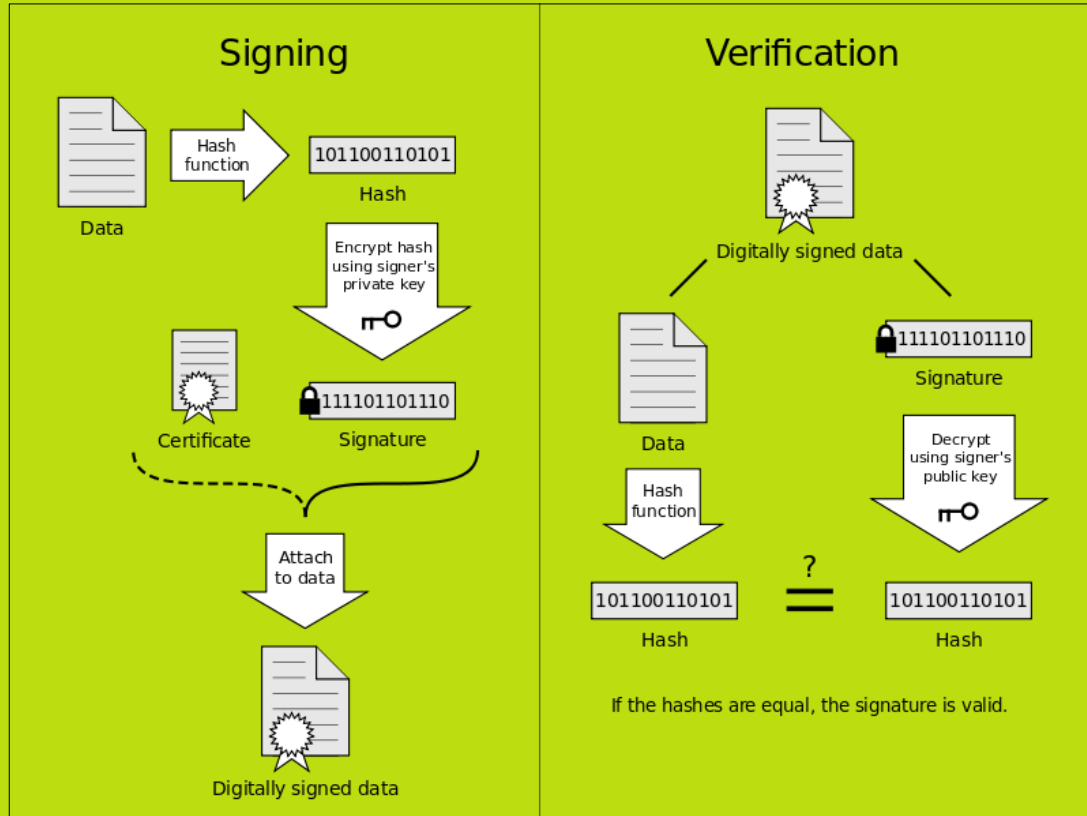
// privater und öffentlicher Schlüssel

// 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 the subject "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, a "Termine" (calendar) sidebar shows 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. A dialog box titled "Konto für eine bestehende E-Mail-Adresse einrichten" is open, displaying the following fields and options:

- Ihr Name:** Vorname Nachname (with a tooltip: "Ihr Name, wie er anderen Personen gezeigt wird")
- E-Mail-Adresse:** ich@example.com (with a tooltip: "Bestehende E-Mail-Adresse")
- Passwort:** Passwort
- ☒ Passwort speichern

Below the fields, it states: "Einstellungen wurden bei Ihrem Anbieter des E-Mail-Diensts gefunden".

There are two radio buttons for storage settings:

- ☒ IMAP (Nachrichten auf dem Server speichern)
- ☐ POP3 (Nachrichten auf diesem Computer speichern)

Server and username information is listed:

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

At the bottom of the dialog are buttons: "Neue E-Mail-Adresse erhalten...", "Manuell bearbeiten", "Fertig", and "Abbrechen".

The background shows the Thunderbird main window with a sidebar on the left containing "Konten", "E-Mail", "Chat", and "Neu". The main pane displays a calendar view for December 2018, showing a "Neuer Termin" (New Event) for "Heute" (Today) and "Morgen" (Tomorrow).

The Windows taskbar at the bottom shows the Start button, search bar, and several application icons. The system tray on the right indicates the time as 15:40 on 09.12.2018.





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.

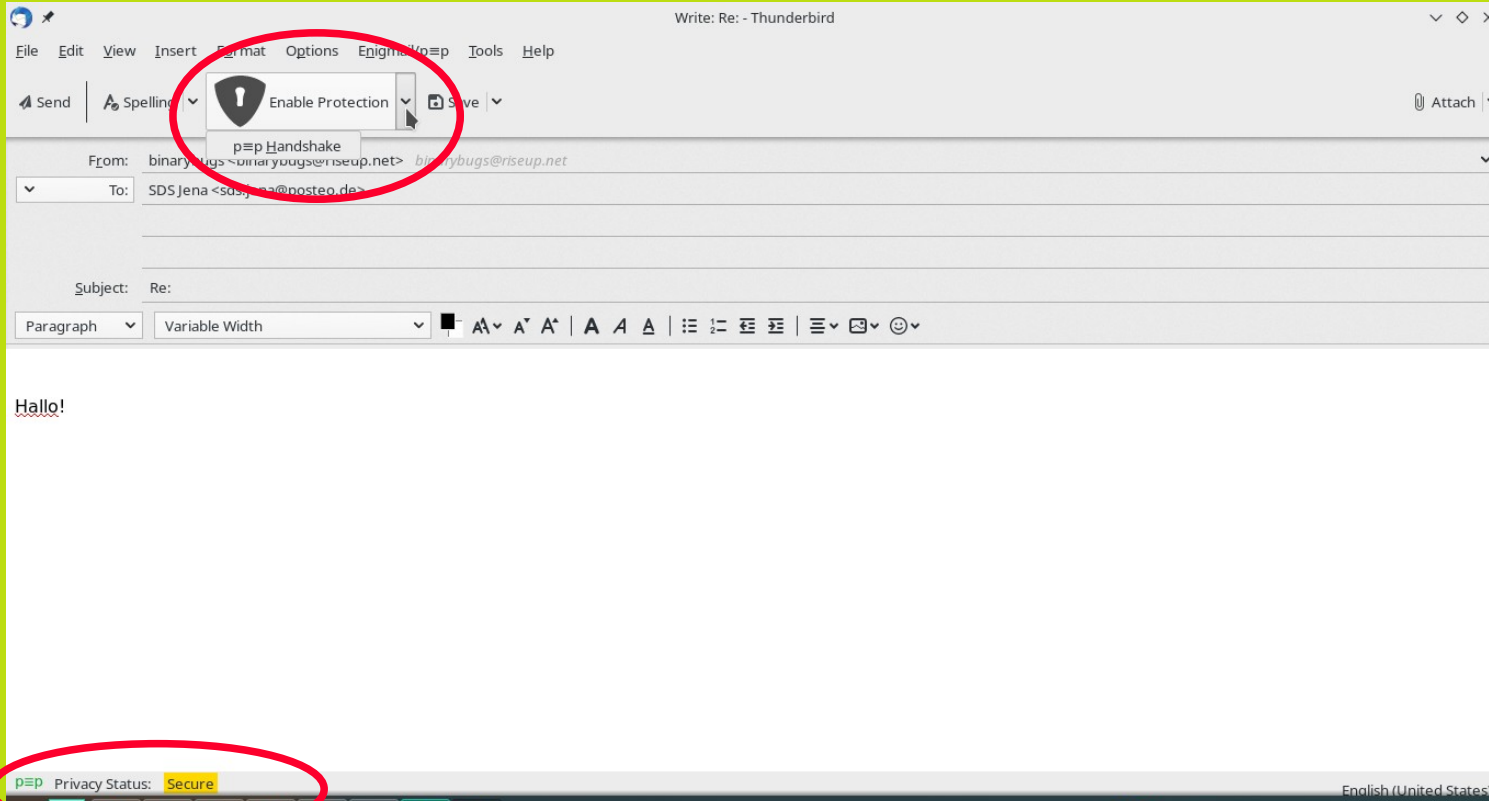
Name	Version	Date	Size	Tarball	Signature
GnuPG	2.2.11	2018-11-06	6406k	<a href="#">download</a>	<a href="#">download</a>



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'. 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.' The left sidebar contains filter options under 'Filterergebnisse', including 'KATEGORIE' (Alle Add-ons), 'FUNKTIONIERT MIT' (Alle Versionen von Thunderbird, Alle Systeme), and 'SCHLAGWORT' (Alle Schlagwörter). 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 the URL 'https://addons.thunderbird.net/thunderbird/downloads/latest/enigmail/addon-71-la'. The dialog has 'Jetzt installieren' and 'Abbrechen' buttons. The background shows the 'Enigmail' add-on details, including a description: 'This module allows you to change/edit email subjects' and a rating of 4.5 stars from 9,041 users. Below it, the 'Mail Redirect' add-on is visible with a description: 'Erlaubt das Umleiten von E-Mails zu anderen Empfängern' and a rating of 4.5 stars from 36,526 users. The right sidebar shows a calendar for December 9th, 2018, with a 'Termin' section. The bottom of the screen shows the Windows taskbar with the search bar and various application icons.



# Und jetzt?



p≡p





# Ran an die Rechner!





## 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:

// cryptoparty.in

// ...



**Danke für eure Aufmerksamkeit!**

