

Cyberselbstverteidigung Kryptografie - das letzte Bollwerk der Privatsphäre?

Mattis
Yannik

19. Januar 2018

Wir sind

- ▶ **Yannik**

- ▶ 25, Master Student der Physik („Complex Systems“)
- ▶ Mitglied beim CCCHB

- ▶ **Mattis**

- ▶ 24, Arbeitet beim DLR („Embedded System“)
- ▶ Mitglied beim CCCHB

Thema: Kryptografie

- ▶ Was ist Kryptografie?
 - ▶ Klartext nach einem bestimmten Muster bearbeiten, sodass Dritte ihn nicht lesen können

Thema: Kryptografie

- ▶ Was ist Kryptografie?
 - ▶ Klartext nach einem bestimmten Muster bearbeiten, sodass Dritte ihn nicht lesen können
- ▶ Wie funktioniert Kryptografie?
 - ▶ Verschiedene Verfahren; früher mechanisch, heute auch elektronisch.

Thema: Kryptografie

- ▶ Was ist Kryptografie?
 - ▶ Klartext nach einem bestimmten Muster bearbeiten, sodass Dritte ihn nicht lesen können
- ▶ Wie funktioniert Kryptografie?
 - ▶ Verschiedene Verfahren; früher mechanisch, heute auch elektronisch.
- ▶ Warum brauche ich Kryptografie?
 - ▶ Privatsphäre, Online-Banking, Demonstration organisieren, (Drogen kaufen)

Inhaltsverzeichnis

Historie der Kryptografie

Aktuelle Gesetzeslagen

Verschlüsselung in der Praxis

Verschlüsselungsstab der Griechen



Caesar Chiffre

Beispielbild:

yannik $\xrightarrow{\text{caesar1}}$ *zboojl* $\xrightarrow{\text{caesar25}}$ *yannik*

Enigma



Enigma

- ▶ Enigma wurde nach und nach „geknackt“.

Enigma

- ▶ Enigma wurde nach und nach „geknackt“.
- ▶ Enigma war uA kriegsentscheidend.

Enigma

- ▶ Enigma wurde nach und nach „geknackt“.
- ▶ Enigma war uA kriegsentscheidend.
- ▶ Sehr fortschrittliche Technologie für die 30/40er Jahre.

Kryptografie in der heutigen Zeit



Abbildung : Symbolbild

Was sollte alles verschlüsselt werden?

- ▶ Kommunikation (Chat, Mail, Telefonat)
- ▶ Überweisungen (!)
- ▶ Funktüröffner/Schließtechnik (Autotür, Firmentür)
- ▶ Firmengeheimnisse
- ▶ Backups
- ▶ Kontaktloses Bezahlen (NFC)

Aktuelle Gesetzeslage in Deutschland

- ▶ Vorratsdatenspeicherung (Internetprovider(Telekom, 1und1,...) müssen Verbindungsdaten speichern). (Im Moment glücklicherweise ausgesetzt)

Aktuelle Gesetzeslage in Deutschland

- ▶ Vorratsdatenspeicherung (Internetprovider(Telekom, 1und1,...) müssen Verbindungsdaten speichern). (Im Moment glücklicherweise ausgesetzt)
- ▶ Staatstrojaner (Behörden bringen Überwachungssoftware auf die Geräte des Beschuldigten.)

Aktuelle Gesetzeslage in Deutschland

- ▶ Vorratsdatenspeicherung (Internetprovider(Telekom, 1und1,...) müssen Verbindungsdaten speichern). (Im Moment glücklicherweise ausgesetzt)
- ▶ Staatstrojaner (Behörden bringen Überwachungssoftware auf die Geräte des Beschuldigten.)
- ▶ Cyberminister wollen Sicherheitslücken nicht melden, sondern „für sich/Dienste“ behalten.

Aktuelle Gesetzeslage in Deutschland

- ▶ Vorratsdatenspeicherung (Internetprovider(Telekom, 1und1,...) müssen Verbindungsdaten speichern). (Im Moment glücklicherweise ausgesetzt)
- ▶ Staatstrojaner (Behörden bringen Überwachungssoftware auf die Geräte des Beschuldigten.)
- ▶ Cyberminister wollen Sicherheitslücken nicht melden, sondern „für sich/Dienste“ behalten.
- ▶ Cyberminister wollen Firmen zwingen Hintertüren einzubauen.

Aktuelle Gesetzeslage in Deutschland

- ▶ Vorratsdatenspeicherung (Internetprovider(Telekom, 1und1,...) müssen Verbindungsdaten speichern). (Im Moment glücklicherweise ausgesetzt)
- ▶ Staatstrojaner (Behörden bringen Überwachungssoftware auf die Geräte des Beschuldigten.)
- ▶ Cyberminister wollen Sicherheitslücken nicht melden, sondern „für sich/Dienste“ behalten.
- ▶ Cyberminister wollen Firmen zwingen Hintertüren einzubauen.
- ▶ Passwörter müssen nicht herausgegeben werden.

Blick auf andere Staaten

- ▶ England hat restriktive Gesetzgebung. (Politik verbietet harte Kryptographie [citation needed])

Blick auf andere Staaten

- ▶ England hat restriktive Gesetzgebung. (Politik verbietet harte Kryptographie [citation needed])
- ▶ In China wird die Privatsphäre kontrolliert (Social Scoring) und Zugang zu Informationen blockiert [citation not needed]

Blick auf andere Staaten

- ▶ England hat restriktive Gesetzgebung. (Politik verbietet harte Kryptographie [citation needed])
- ▶ In China wird die Privatsphäre kontrolliert (Social Scoring) und Zugang zu Informationen blockiert [citation not needed]
- ▶ Frankreich: Notstand (seit 13.Nov 2015) und Anti-Terrorgesetze.

Grundprinzip und Methoden

- ▶ Welches Grundprinzip steckt dahinter?
 - ▶ symmetrische Verschlüsselung (wie eine Schatzkiste mit 2 Schlüsseln)
 - ▶ asymmetrische Verschlüsselung (einer hat das Schloss, der Andere den Schlüssel dazu)

Kleines Beispiel - 1

Von dem folgenden müsst ihr nicht alles verstehen, das macht „das Programm“ alles für euch.

Schlüsselerzeugung behandeln wir später, hier nur ein Schlüsselpaar

Privater Schlüssel: $\{d = 47\}$

öffentlicher Schlüssel: $\{e = 23, n = 143\}$

Kleines Beispiel - 2 (Ver- und Entschlüsselung)

Nachricht m soll verschlüsselt versendet werden, dazu wird c berechnet und versendet (mod ist die Modulo Operation, besser bekannt als „Rest“ einer Division)

$$c = m^e \text{ mod}(n) \quad (1)$$

Zur Entschlüsselung wird m aus c berechnet:

$$m = c^d \text{ mod}(n) \quad (2)$$

Kleines Beispiel - 2 (Ver- und Entschlüsselung)

Nachricht m soll verschlüsselt versendet werden, dazu wird c berechnet und versendet (mod ist die Modulo Operation, besser bekannt als „Rest“ einer Division)

Wir versenden eine Nachricht „7“

$$c = m^e \text{mod}(n)$$

$$c = 7^{23} \text{mod}(143) = 2$$

2 wird versendet.

Zur Entschlüsselung wird m aus c berechnet:

$$m = c^d \text{mod}(n)$$

$$m = 2^{47} \text{mod}(143) = 7$$

cool.

Einrichten von ENIGMAIL in Thunderbird

The screenshot shows the Thunderbird Add-ons Manager window. The search bar at the top contains the text "Enigmail". The "Suchen" (Search) sidebar on the left is visible. The main list of add-ons includes:

- Enigmail** (highlighted with a red box): Verschlüsseln und Authentifizieren von Nachrichten mit OpenPGP. Basiert auf GnuPG (www.gnupg.org). Mehr... Installieren
- Mail Merge**: Mass Mail and Personal Mail. Mehr... Installieren
- Mail Redirect**: Erlaubt das Umleiten von E-Mails zu anderen Empfängern. Mehr... Installieren
- EditEmailSubject (Edit email Subject)**: This module allows you to change/edit email subjects. Mehr... Installieren
- Expression Search / GmailUI**: Powerful message searching through expressions. Type "from:fred to:tom" to see all messages from Fred to Tom in the current view. Supp... Mehr... Installieren
- Mailbox Alert**: Mailbox Alert allows you to specify, for each separate mail folder, a message, sound and/or a system command that will be executed wh... Mehr... Installieren
- Mail Summaries**: Adds a summary of mail accounts and folders to replace the account central pane and the empty folder preview. Mehr... Installieren
- BIDI Mail UI**: Direction control and BIDI-related charset misdetection correction. Mehr... Installieren
- Expand mailing list recipients**: Fügt einen Toolbar-Button hinzu, über den Adressbuch-Listen in denen Empfänger aufgelistet werden - hilfreich, wenn einzelne Empfänger... Mehr... Installieren
- Get Selected Mails**: Gets new messages for selected mail accounts. Mehr... Installieren
- GmailOutOfOffice**: Out of Office for Gmail! This add-on allows you to set an out of office auto-responder in your gmail account. It adds a button in the toolbar... Mehr... Installieren

At the bottom of the list, there is a link: [Alle 118 Ergebnisse anzeigen](#)

The Windows taskbar at the bottom shows the date and time as 12:50 on 14.01.2014.

Einrichten von ENIGMAIL in Thunderbird

The screenshot shows the Thunderbird interface with the Enigmail 1.9.9 add-on page. The page title is "Enigmail 1.9.9 (deaktiviert)" by Patrick Brunschwig. It features a green status bar at the top indicating that Enigmail is installed but deactivated. The main content area contains text about OpenPGP encryption and authentication, a note about the add-on's status, and a call to action to support the developer. A table at the bottom provides metadata such as the last update date (14. Januar 2013), the homepage URL (http://www.enigmail.net/), and a rating of 138 reviews.

✓ Enigmail wird installiert, sobald Sie Thunderbird neu starten. [Jetzt neu starten](#) [Rückgängig](#)

Enigmail 1.9.9 (deaktiviert)

Von [Patrick Brunschwig](#)

OpenPGP message encryption and authentication

Enigmail integriert OpenPGP-Verschlüsselung und Authentifizierung in Thunderbird und Seamonkey. Dabei stellt Enigmail die Benutzeroberfläche zur Verfügung, während die Verschlüsselung selbst von GnuPG (www.gnupg.org) im Hintergrund vorgenommen wird. Enigmail bietet automatische Ver- und Entschlüsselung an, sowie eine grafische Oberfläche zur Verwaltung von Schlüsseln.

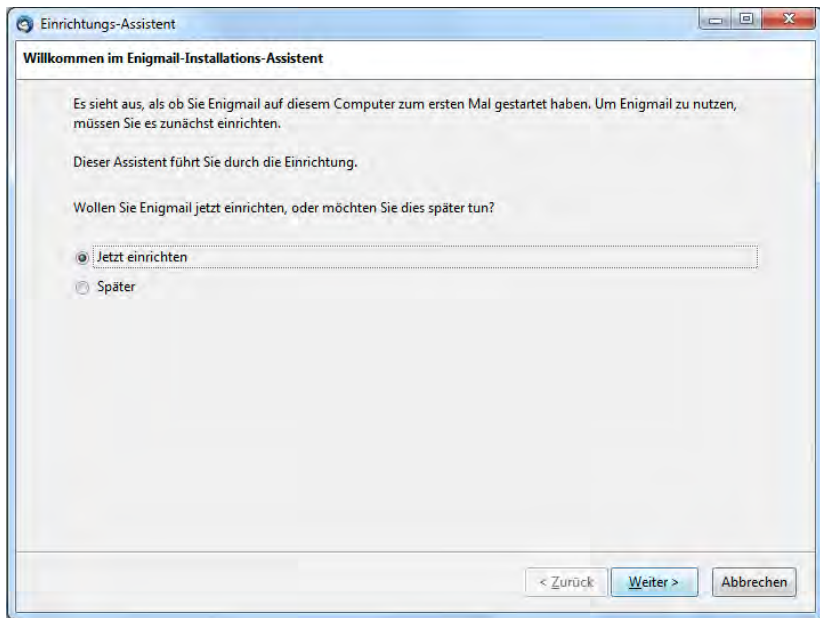
Anmerkung: GnuPG ist nicht Teil von Enigmail, wird aber bei Bedarf automatisch installiert.

Der Entwickler dieses Add-ons bittet Sie, das Sie die Entwicklung unterstützen, indem Sie einen kleinen Betrag spenden

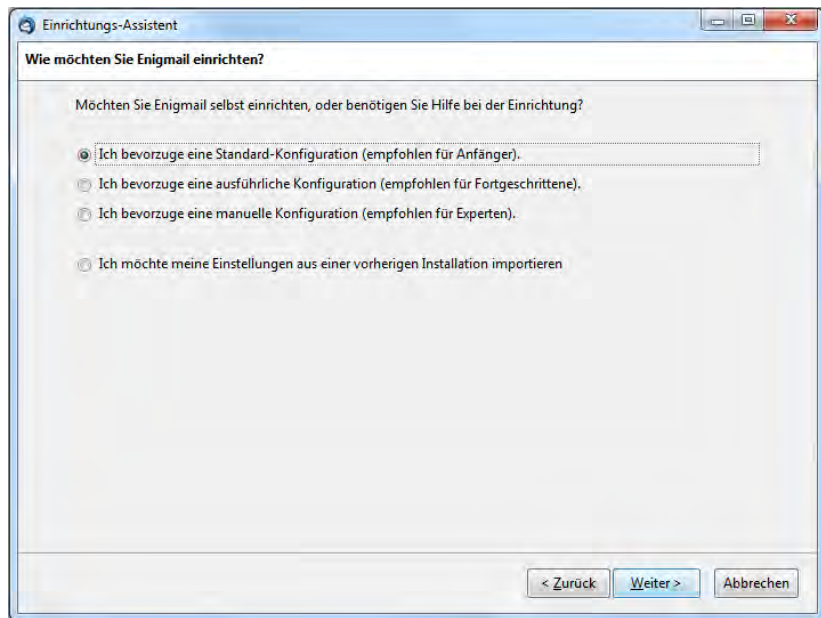
[Spenden](#)

Zuletzt aktualisiert	14. Januar 2013
Homepage	http://www.enigmail.net/
Bewertung	★★★★☆ 138 Bewertungen

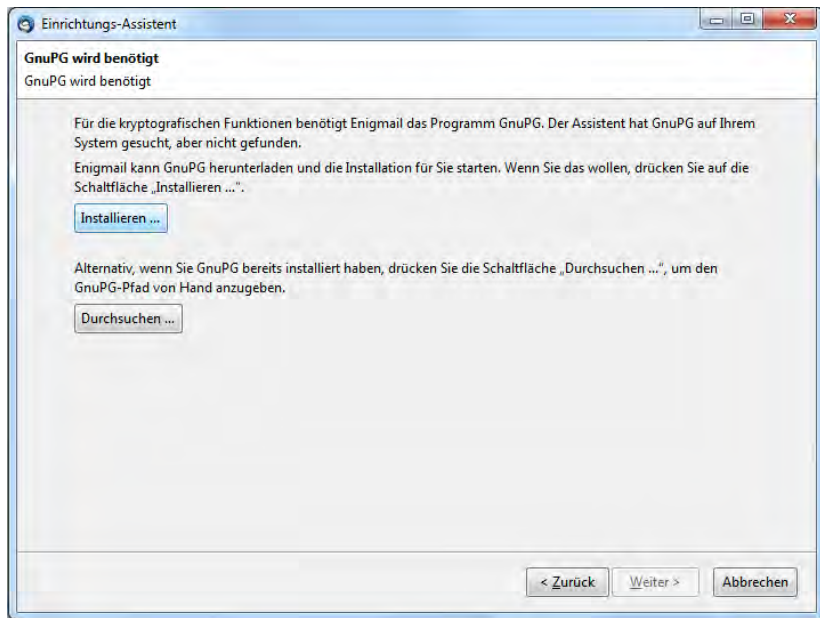
Einrichten von ENIGMAIL in Thunderbird



Einrichten von ENIGMAIL in Thunderbird



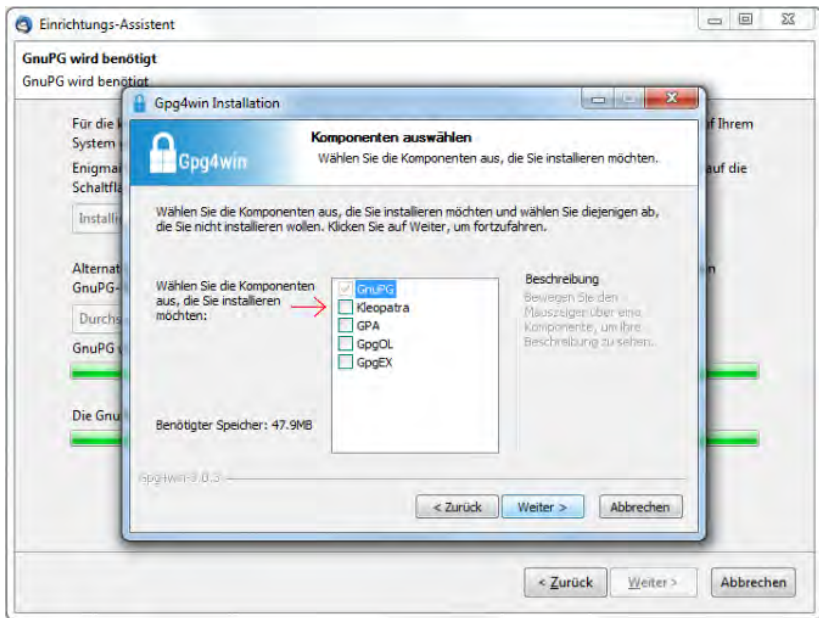
Einrichten von ENIGMAIL in Thunderbird



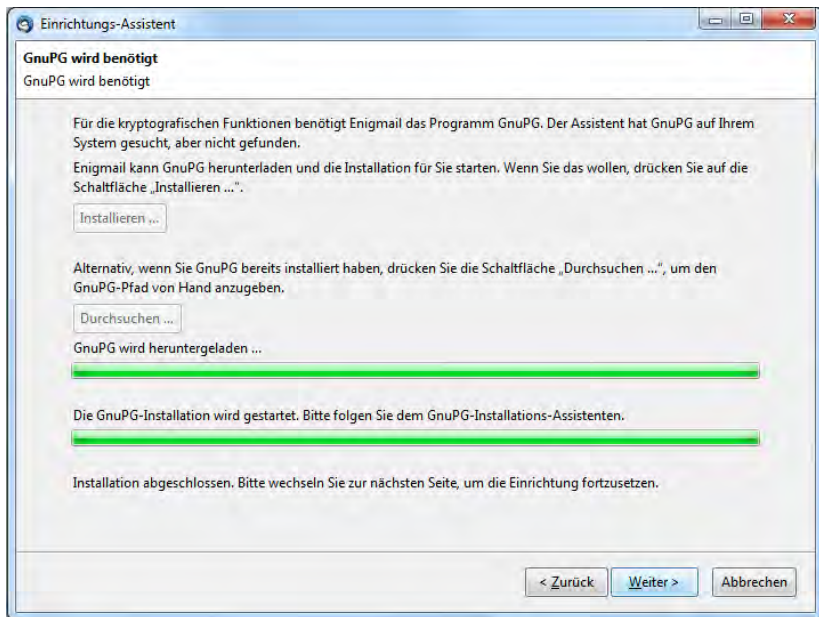
Einrichten von ENIGMAIL in Thunderbird



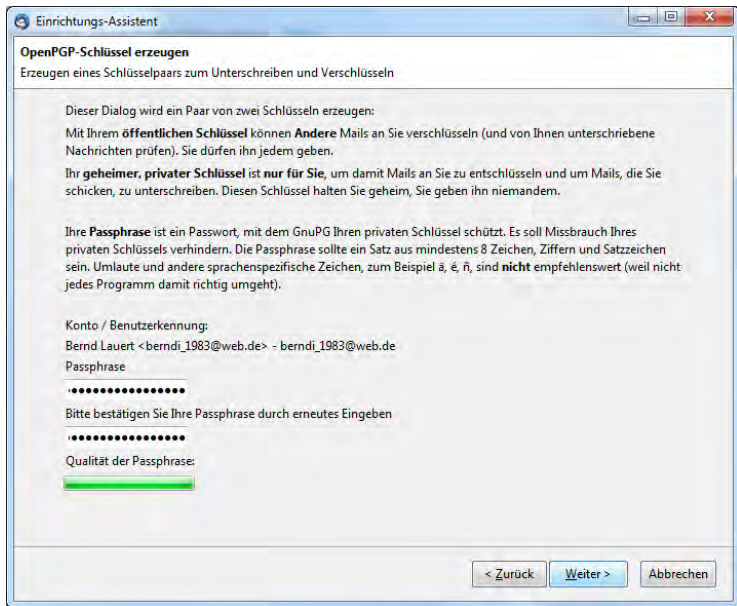
Einrichten von ENIGMAIL in Thunderbird



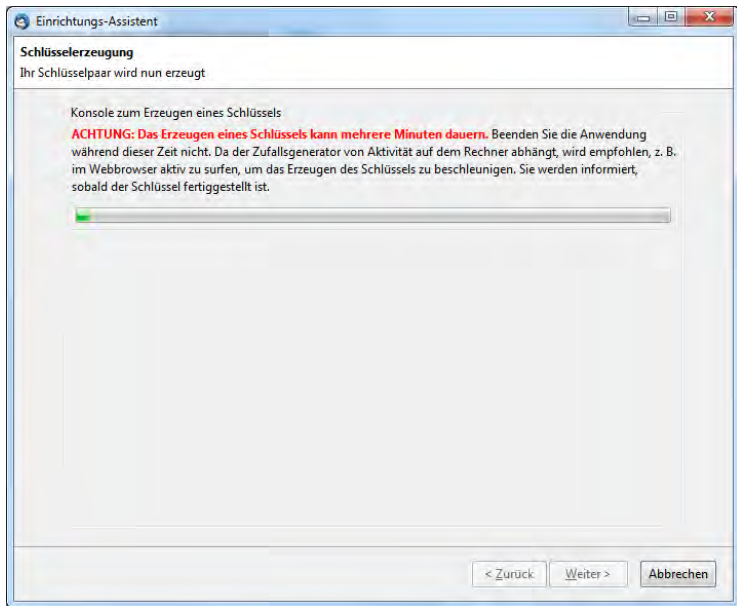
Einrichten von ENIGMAIL in Thunderbird



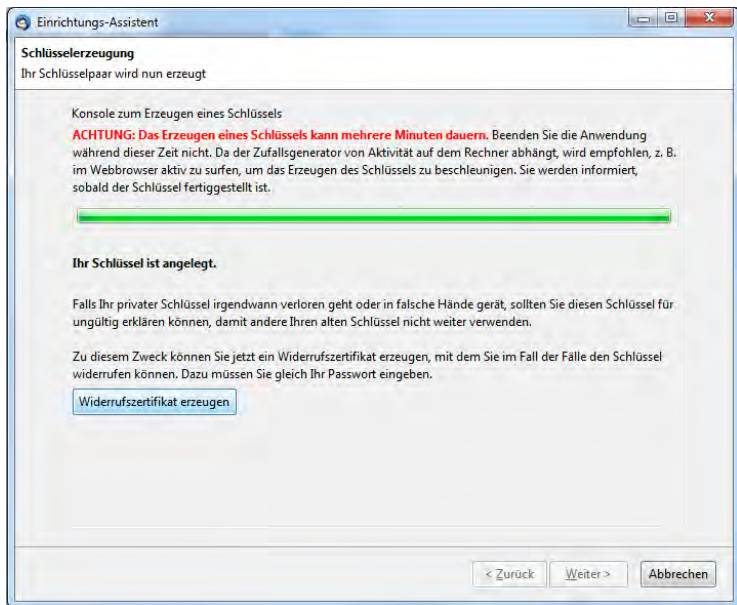
Einrichten von ENIGMAIL in Thunderbird



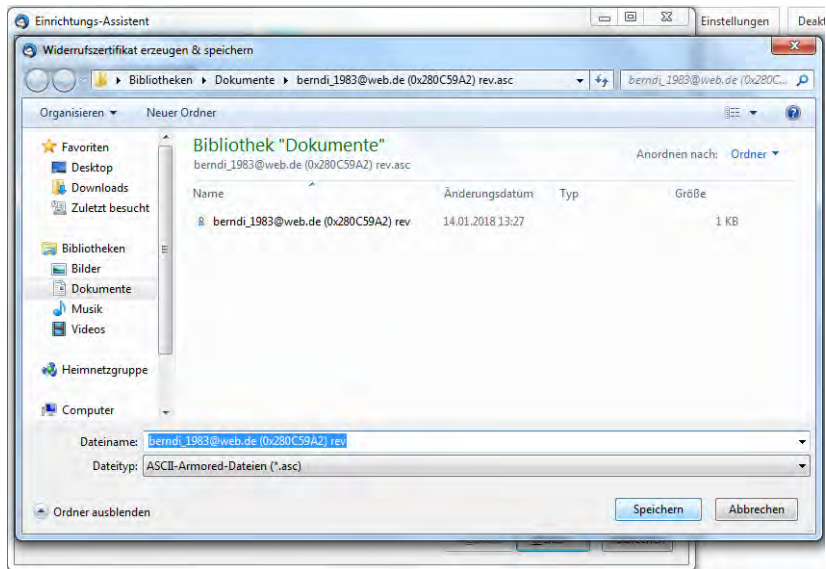
Einrichten von ENIGMAIL in Thunderbird



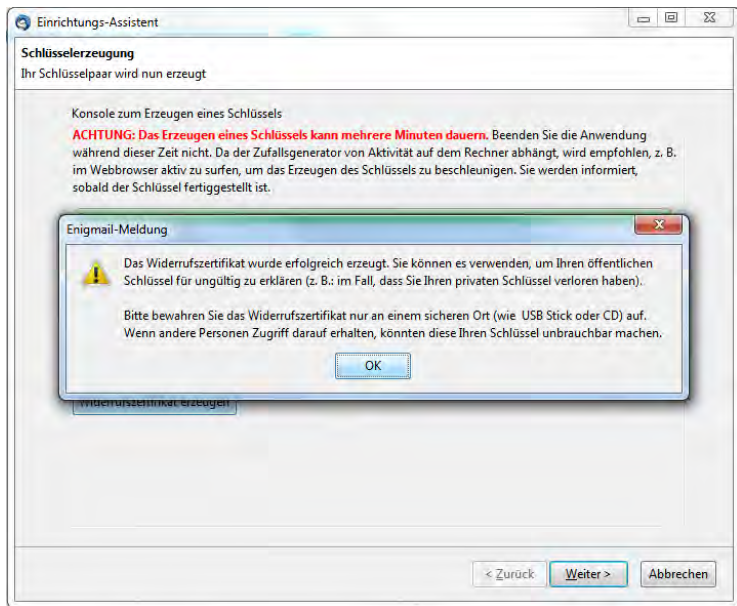
Einrichten von ENIGMAIL in Thunderbird



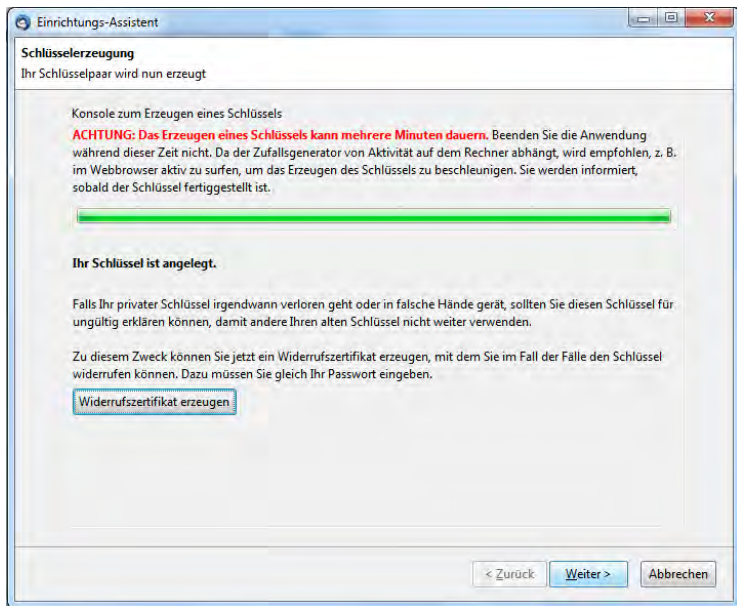
Einrichten von ENIGMAIL in Thunderbird



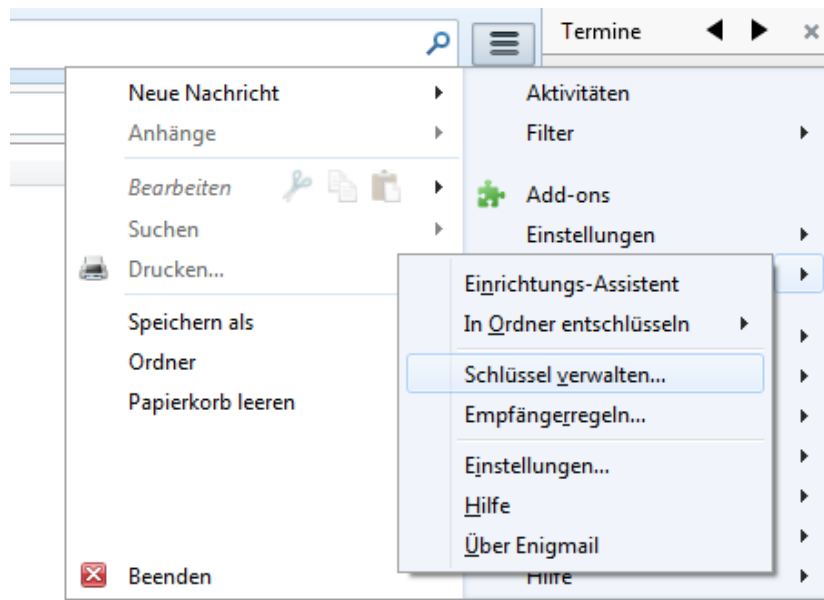
Einrichten von ENIGMAIL in Thunderbird



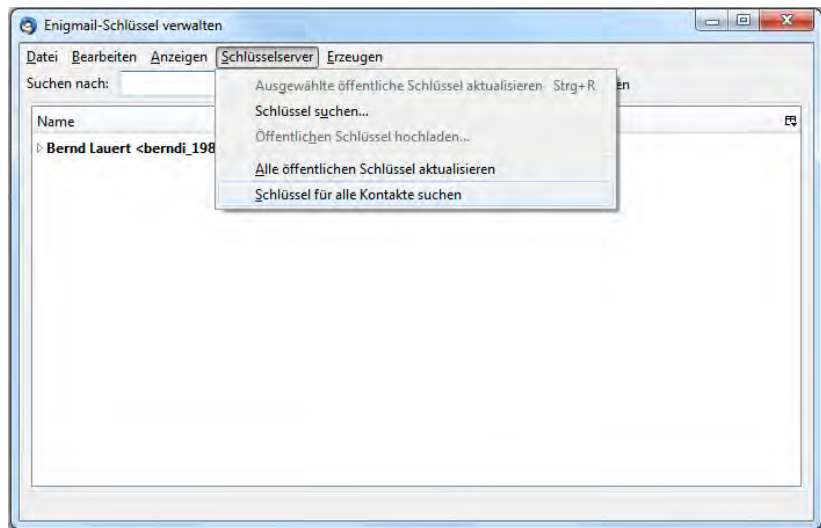
Einrichten von ENIGMAIL in Thunderbird



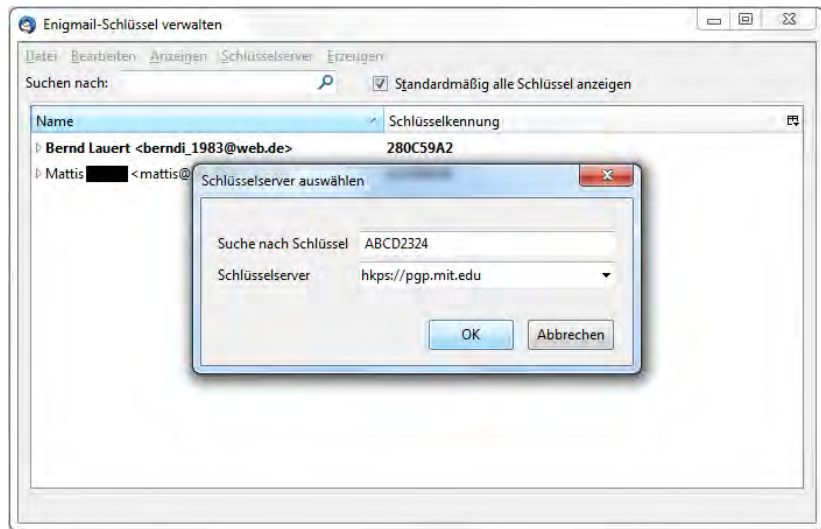
Einrichten von ENIGMAIL in Thunderbird



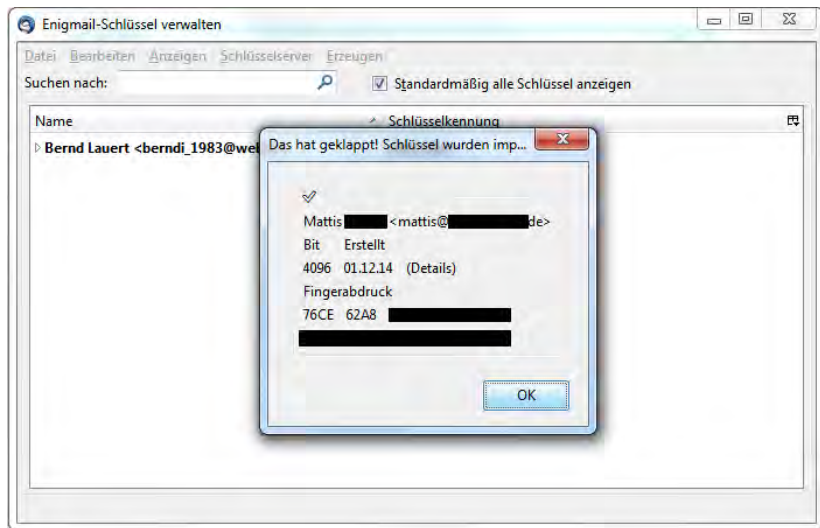
Hinzufügen eines Schlüssels mit ENIGMAIL in Thunderbird



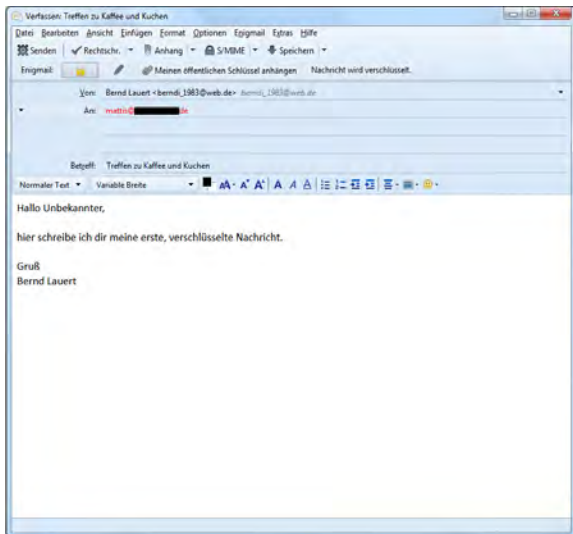
Hinzufügen eines Schlüssels mit ENIGMAIL in Thunderbird



Hinzufügen eines Schlüssels mit ENIGMAIL in Thunderbird



Schreiben einer verschlüsselten Nachricht mit ENIGMAIL in Thunderbird



Quelltext einer verschlüsselten Nachricht

```
Quoted text was hidden because it is longer than 10000 characters.
Date: Wednesday, 24 Jun 2015 13:46:43 +0100
From: Bernd Lauret <bernd_l19@web.de>
Subject: Treffen zu Kaffee und Kuchen
Message-ID: <baad6b0b-4d31-b6b8-53c154c90326b45@web.de>
Date: Sun, 14 Jun 2015 13:46:43 +0100
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; rv:52.0) Gecko/20100101
Thunderbird/52.1.3
MIME-Version: 1.0
Content-Type: multipart/encrypted;
  protected="application/pgp-encrypted";
  boundary="75a641e95PTkUp5R8K3QBjvCNEVh3jY"

This is an OpenPGP/MIME encrypted message (RFC 8980 and 3156)
--75a641e95PTkUp5R8K3QBjvCNEVh3jY
Content-Type: application/pgp-encrypted
Content-Description: PGP/MIME version identification

Version: 1

--75a641e95PTkUp5R8K3QBjvCNEVh3jY
Content-Type: application/octet-stream; name="encrypted.asc"
Content-Description: OpenPGP encrypted message
Content-Disposition: inline; filename="encrypted.asc"

-----BEGIN PGP MESSAGE-----

NQ4Wx11fWwL6amQj/S6P5d6cAicV1tq6w4o4:Fnq3No0u4L8EtVr3S+eB3j
E2w6D0n08Llg7+eU1XQFhZcW1L578A54137mua+M0S:BTZg6S3L5pVPLA
8KcU1w6c1+re4qfQwK2Z23D08B05L1KFPf9d6U0u4uW7Yq5i0S7pDQ
8KxL6BhWgqfK5dY4W02U596u+7xy0f15kY3hK1h4B446213YV
90cM5q2at0MAuMdp0Tfcc2Sustyh4s1FvY1SP7T3AICR6e20G148Tj0f
QWVF8B81Fv7HGFVACTuulq6t4eKsagr7jgE4L1W0uYyJgk+wB115cPK
1z0P5C2Q6wLew1Juc24w6Q74bYv8BurdUvYf18YfYz5P80Uc1L+
DerburjK24HQ0T79n0C83u4H7zvgp4YxU6j8YyU6Jk4uPh7uWv+8Yy18X
1cTULtAgC6bWv/ABRuE165X3L1924WPKZgawofAq70G6L1276633P9W0q
811g866t/cK7h3pT41S0/y0H4QzRqj0v7KIC0IQj6wGqzJKZ060CFFgff
cFf8GfP7er4wK11Fw6N7W4Lm0T4g6KcV+1Cj5r8r75002w3J1CDDF
AqD+8Bp4p0t808RO/LM5P4uq4t0q09p4e046014K1v0i+R37V1NaurvP48
418R0W68Y821y1CLmW4yglRQ4qFvE7Y7Y15q:1p44+Y36Agg0n8W8
8Yv2D+6Q28Lz+uPl0fC6h3L6ary1L230038:007pF6uK109u6L1e1F8q6
w6b5yF4g4X0011FvU11u4v5F613g7r4uK3Pw4uF4T01L4q6u478
ky8Zw6X34h4uT4V01CvK/vhCz/sFpC6U0y37m4u4v+q661EAD9j0y6wE
MGB8C14uKfpx+Q8P+Vv1.d0e7P0tAupw8PQZ9Y8B3c407EvY24Y6m5/1JF
9w6h5Pm61L16u8X+1uVC6qF75c46405Zf+u4+1Tq6L20u4f7hg4uY
Drt+v6u4uF29+K2Ac1uV7h4g6c3w42Zf9YvF4F71L2U19NhgL4u62J6/
0Q/w4S7J034/h6yKfrc2wC6P788j3HC736R0q4U5G5u0Q4uW0u2Lc
fCP4b05u3y8y5b6r4e8A7F0T2a05153Q0W765mb+44w37u8B72j2t4vFfE
Qm+u4p02L1+8g761u4/0u4P2Z212035m4PZAL1vUy7h0QC7u4B
Fut20w4uq34Mz1c15F8W4q5G4M4KXov1+4w44uq4v018B00K3qP1t4
340K1781Kf810C4K1scFk787+R046776u46s42qee4E4Dn10F496E3K4wK
R1j2w4u6d4u98g8V7L46y64u464724214674yQc40m4070mP6m46q
w4b1VYv4v4u45g4v4m43g4v24b4u4g4C431v4u49451522+4u464u4m4
UP+u4u4b4374u4v4u4R434F4C4v4Q4C4Q4m4M4u4c4y4u4d41C4L4514j4k
M354M4j734X4+4646v4v4f7F4u47J4Q4J03121L0719U41R4U44+5646493v41
p4D6w4z4124V4u4q4v4+00g24/204K4g48v47b464u43f46413j4c4+54L4
```

Quelltext einer verschlüsselten Nachricht

```
Quoted text follows:-----
Date: Berkeley: groch: zsh
1:hsd41eh3PTkudp5A8K30BhJcNfVhjYr
MIME-Version: 1.0
Content-Type: multipart/encrypted;
protocol="application/pgp-encrypted";
boundary="75a841eh3PTkudp5A8K30BhJcNfVhjYr"

This is an OpenPGP/MIME encrypted message (RFC 4880 and 3156)
--75a841eh3PTkudp5A8K30BhJcNfVhjYr
Content-Description: OpenPGP encrypted message
Content-Type: application/pgp-encrypted
Content-Description: PGP/MIME version identification

Version: 1

--75a841eh3PTkudp5A8K30BhJcNfVhjYr
Content-Type: application/octet-stream; name="encrypted.asc"
Content-Description: OpenPGP encrypted message
Content-Disposition: inline; filename="encrypted.asc"

-----BEGIN PGP MESSAGE-----

hQdMx1j1rrk6arqQ/9GMSdbcaKv1tGurWuad;FaqjNoofuo4EhTfV35wd33
8pdx0D0uH8Iqz7+eUd1XQFNDcW7I8279H4b137m4A0K5cBT0g053513npVKA
8pdx0u0ed+Lrre3jQdWV0Z258D0h0w118F9f9p0k00k0u0u0WfYjQ5m703D0
0kYx0d0u0k0g0f0k0k0u0002500k0u037y0Yf31kYk0k0k1H0d0u0d3EYf
90C0k0j2at0D0u0A0p0Tf0c25u0tYh0e5fYjL5P7230A1C0R0r20G8j04Tj0T
0uV0f080u0r0730R0F0W0T0u0g0f0k0k0g0f7jE0kX0Y0u0v0j0y0k0w0d015fR0
110P0C0Z0d0u0L0ed1J0u020d0Q0T0H0Y050d0U0v0L0R0Y0f0J0R00c1L0
D0r0u0r0Q0v0C0T0M0C0B0u0H70u0g04Y0u0l0Y05Y06J0u0A0F0u0W0f0Y0X
1c7E0u030c0w0m0A0R0u0E0k0X3119240u0R0Z0g0u0A0P0G0L175633P0W0Q
811j0d0d0r0c0k0h0p0t0S0r0y00K0Q0R0p0j0v0T0C0I0Q0B0u0g0z0k02060C0F0g0F
c0F0G0P0T0v0r0k0L1F0A0C0E0W10c0Z0g0K0c0+L030y0R075000w0731X0D0
A0u00B0p0d0p080d0u0H0F0A0g0k0T0o090e0d0A0h0K10v0310c0V0u0r0u0W
41R0K0u0y0W21v0j1C0u0h0A0y0jR0M0q0F0E0T0Y0j0y03p0A0V30A0g0u0n050w
0kY0j0+0Q0Z0j0u0p0G0C0B0L0A0Y0t0309030r0070P0f0e0k010V0u030e1F0g0
0w0e0d0Yf040g0d0u10k0j10k0u0F0k0j0r0j0g0u0d0W0h0w0f0D010A0p0a0706
kY820u0W30M0u0T0V01C0K0r0V0C0r0R0y0y070u0A0V0+0g0c0E0B0j0g0y0w0C
0d080C10k0jY0x0Q0v0u0d0e070E0A0u0u0P0Q0Y0B0r0u0F0v0y0Z0u0m0s0j0Jf
0w0h0r0m0L10S0B0k0+0u0V0Q0P050d00C0y0Z0u0e0L070g0k120u0F0f0g0u0V
D0r0v0p0u0e0F20+020A0c0L0u0H0k0g0j0w02J0K0y0V040F7310V070P0g0u0k0Z0
0Q0w0K370j0+0y0w0C0F0u020A0R0P0Bj30R0G0p0U0S0G0u0M0u0N0u0c0L0k
0C0P0u0b0c0B0Y050Y0e0H0A0F0T020c0510S0Q070810h0+0W070u0B0730p0t0v0F0
1Q0w0u0P0D210u0g0E0u0L0u0P0d0P0Z0I0C030u0F0E0L0V0Y0Y0H0Q0C0y0L0R
F0u020u0W0h0j40c0z0L0c05f0B0u0g0g0M0d0K0u0v0+0h0d0u0g0p0c050A0B00u0J0f050
30K0L170E0F0E0C0k050f0K070+0h0g070u0c0u0k0f20u0e0E0D0T10V0P0E03k0e0Z
R0j20w0h0d0u0v080g0B0V10k0y0u0k04020I0F0670u0Y0C0d0h0d0T0M0P0G0g0
0u0b0c0Y0Y0v0e0M030g0v0e0m030r020h0u0d0C0R0j10d0p0S0C2Z0+0d0h0m0P
0P0+0u0d0310h0v0A0R0L0k0P0c0v0G0C0D0u0G0M0n0C0D0Y0u0H0C0E0310f10e0k0
M050k0y0730X0+0h0G0w0r0F0F0u0c0T0F0J0j0j120d070L0W0Q0e050h0g0v0Y
p0d0u0k0z0L0h0Y0k0g0V0+0Q0Z070c0C0g0R0v0P050K0J0Y0H0230c0+0S0c0
+10f0g0h0F0e0L0M0P0g0h0Y0h0P0u0h0c0h0c0h0u0c030k0u010Y0k0k0d0F0g0a
0k0L0u0F0S0E0K0c0310P0F090b07230Y0P0M0u0v0F0G010B07730R0p0c0v0T0u0r
0d0m0180+0d0h0w07h02j0H70h0c0v0w0e0H0G0k048230g0f0u0e0+
+140C

-----END PGP MESSAGE-----

--75a841eh3PTkudp5A8K30BhJcNfVhjYr-----
```


Weitere tolle Tools

- ▶ TrackerBlocker/Adblocker/uBlock im Browser
- ▶ Sichere Messenger (Signal, Threema, [Whatsapp])
- ▶ Backups verschlüsseln mit TrueCrypt/Veracrypt/LUKS

Quellen

- ▶ (Ausnahmezustand in FRA) <https://www.tagesschau.de/ausland/frankreich-notstand-101.html>
- ▶ (VDS)
https://www.bundesnetzagentur.de/DE/Sachgebiete/Telekommunikation/Unternehmen_Institutionen/Anbieterpflichten/OeffentlicheSicherheit/Umsetzung110TKG/VDS_113aTKG/VDS.html
- ▶ (Social Scoring China) [https://de.wikipedia.org/wiki/Sozialkredit-System_\(VR_China\)](https://de.wikipedia.org/wiki/Sozialkredit-System_(VR_China))
- ▶ (Ausnahmezustand Frankreich) <https://netzpolitik.org/2017/frankreich-ausnahmezustand-ohne-ende>

Quellen

- ▶ ENIGMAIL <https://enigmail.net/index.php/en/>
- ▶ (RSA)
<https://de.wikipedia.org/wiki/RSA-Kryptosystem>
- ▶ „Einführung Kryptographie“ von Daniel Steinhauer

Bilder Quellen

- ▶ <http://gayoudesign.blogspot.de/2014/09/cyber-art-wallpaper-hd.html>
- ▶ <https://creativecommons.org>

Danke, danke, dass ihr da wart, kommt zum CCC,
denn er ist sehr gut

Bonusfolie 1 : Security by Obscurity

Bonusfolie 1 : Security by Obscurity

- ▶ (E-Post, Georg Rau) „Grundsätzlich gilt, dass wir hier bei uns keine Sicherheitslücke sehen. Mehr will ich nicht sagen. Denn ein wesentlicher Aspekt unseres Sicherheitskonzeptes ist: Wir reden in der Öffentlichkeit nicht darüber. Das ist Teil des Sicherheitskonzeptes.“

Bonusfolie 1 : Security by Obscurity

- ▶ (E-Post, Georg Rau) „Grundsätzlich gilt, dass wir hier bei uns keine Sicherheitslücke sehen. Mehr will ich nicht sagen. Denn ein wesentlicher Aspekt unseres Sicherheitskonzeptes ist: Wir reden in der Öffentlichkeit nicht darüber. Das ist Teil des Sicherheitskonzeptes.“
- ▶ Bei der „PC-Wahl“ wieder das gleiche Spiel.

Bonusfolie 2 : Die NSA knackt doch eh alles

- ▶ Supercomputer schaffen etwa 100.000 Passwörter pro Sekunde

Bonusfolie 2 : Die NSA knackt doch eh alles

- ▶ Supercomputer schaffen etwa 100.000 Passwörter pro Sekunde
- ▶ Das Jahr hat 31556736 Sekunden.
- ▶ Annahme: Das Passwort besteht aus Groß- und Kleinbuchstaben, sowie Ziffern und ist 20 Zeichen lang. ($62^{20} = 7 \cdot 10^{35}$ Möglichkeiten).

Bonusfolie 2 : Die NSA knackt doch eh alles

- ▶ Supercomputer schaffen etwa 100.000 Passwörter pro Sekunde
- ▶ Das Jahr hat 31556736 Sekunden.
- ▶ Annahme: Das Passwort besteht aus Groß- und Kleinbuchstaben, sowie Ziffern und ist 20 Zeichen lang. ($62^{20} = 7 \cdot 10^{35}$ Möglichkeiten).

$$T = \frac{62^{20}}{100.000 \cdot 31.556.736 \cdot 2} = 10^{23} a$$

Bonusfolie 3 : Schlüsselerzeugung

1. Wähle zwei große Primzahlen: p und q
2. $n = p \cdot q$
3. $\Phi(n) = (p - 1)(q - 1)$
4. Wähle e und d mit der Eigenschaft: $e \cdot d \bmod \Phi(n) = 1$ denn dann ist e teilerfremd zu $\Phi(n)$

Privater Schlüssel: d

öffentlicher Schlüssel: e , n konkret mit Zahlen:

1. Wähle $p = 11$, $q = 13$
2. $n = 11 \cdot 13 = 143$
3. $\Phi(143) = (11 - 1)(13 - 1) = 120$
4. Wähle $e = 23$ teilerfremd zu 120
5. Bestimme d , sodass $23 \cdot d \bmod 120 = 1 \rightarrow d = 47$

Privater Schlüssel: $d = 47$

öffentlicher Schlüssel: $e = 23$, $n = 143$

Bonusfolie 4 : Emails fallen doch unter das Fernmeldegeheimnis

- ▶ Emails fallen prinzipiell unter das Fernmeldegeheimnis, zumindest bei der Übertragung.

Bonusfolie 4 : Emails fallen doch unter das Fernmeldegeheimnis

- ▶ Emails fallen prinzipiell unter das Fernmeldegeheimnis, zumindest bei der Übertragung.
- ▶ Aber Emails können auch von den Behörden beschlagnahmt werden.