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

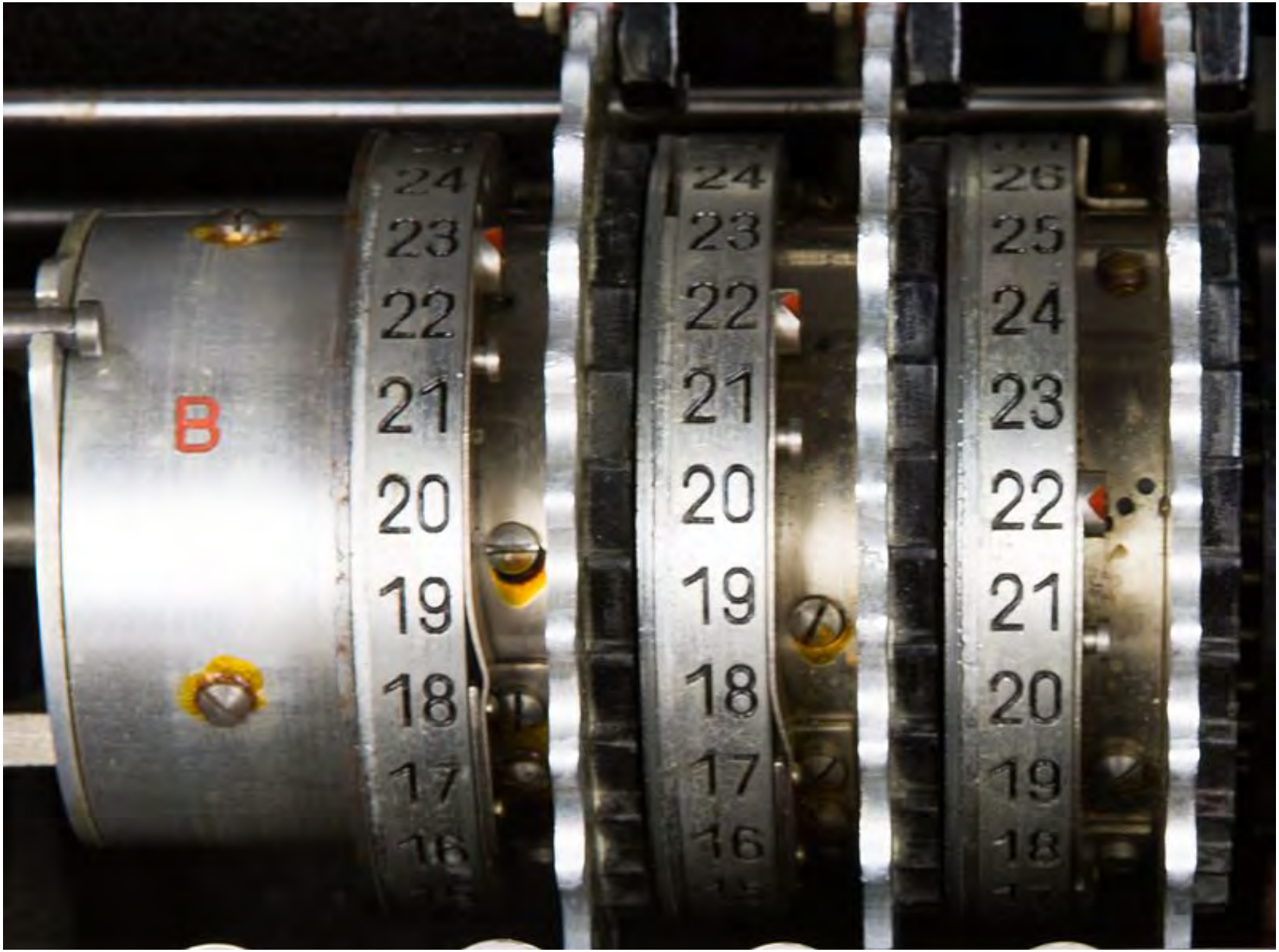
Verschlüsselungsstab der Griechen

Caesar Chiffre

Beispielbild:

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

Enigma


B
24
23
22
21
20
19
18
17
16
24
23
22
21
20
19
18
17
16
26
25
24
23
22
21
20
19
18

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)

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

Zur Entschlüsselung wird m aus c berechnet:

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

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“

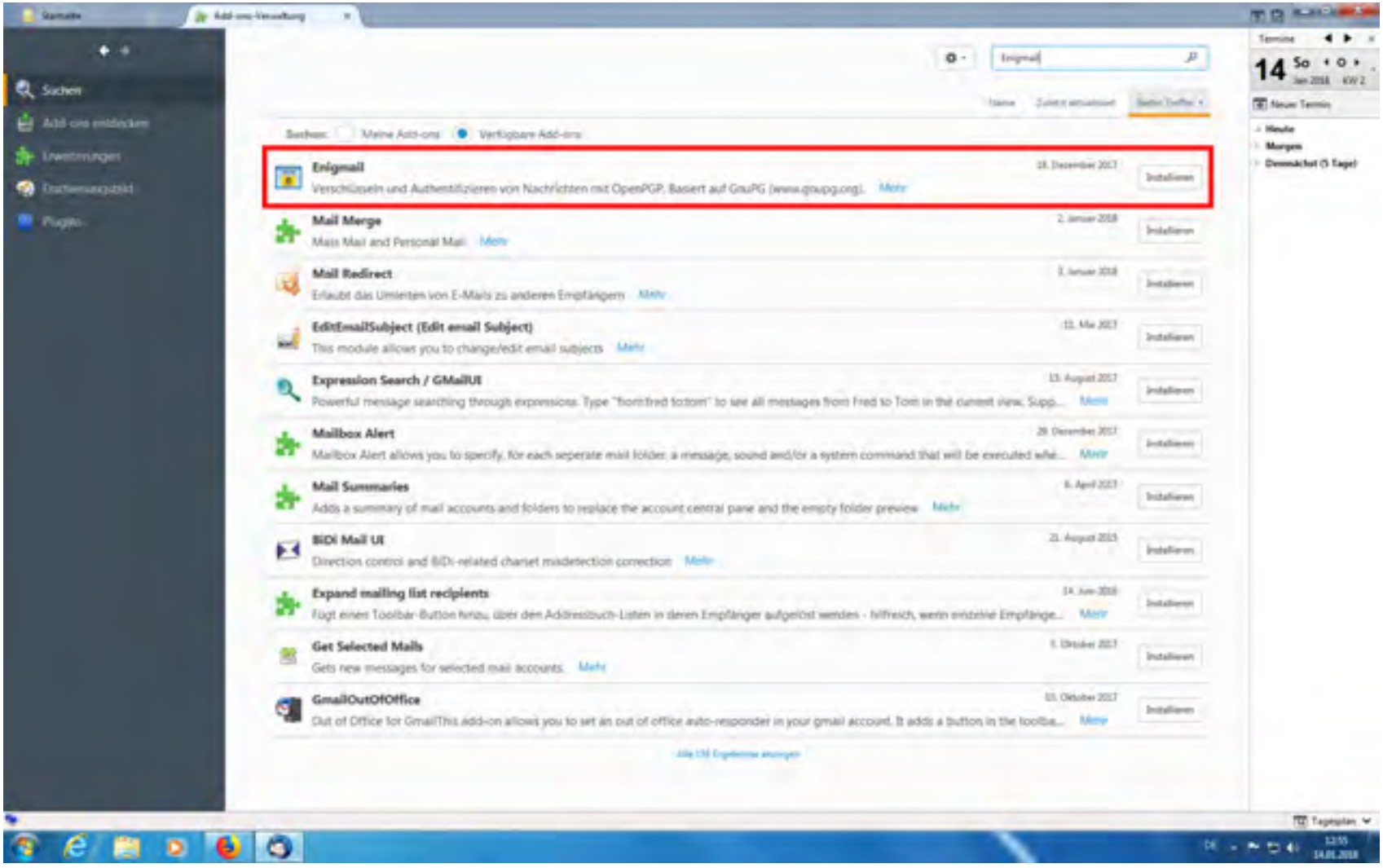
$$c = m^e mod(n)$$
$$c = 7^{23} mod(143) = 2$$

2 wird versendet.
Zur Entschlüsselung wird m aus c berechnet:

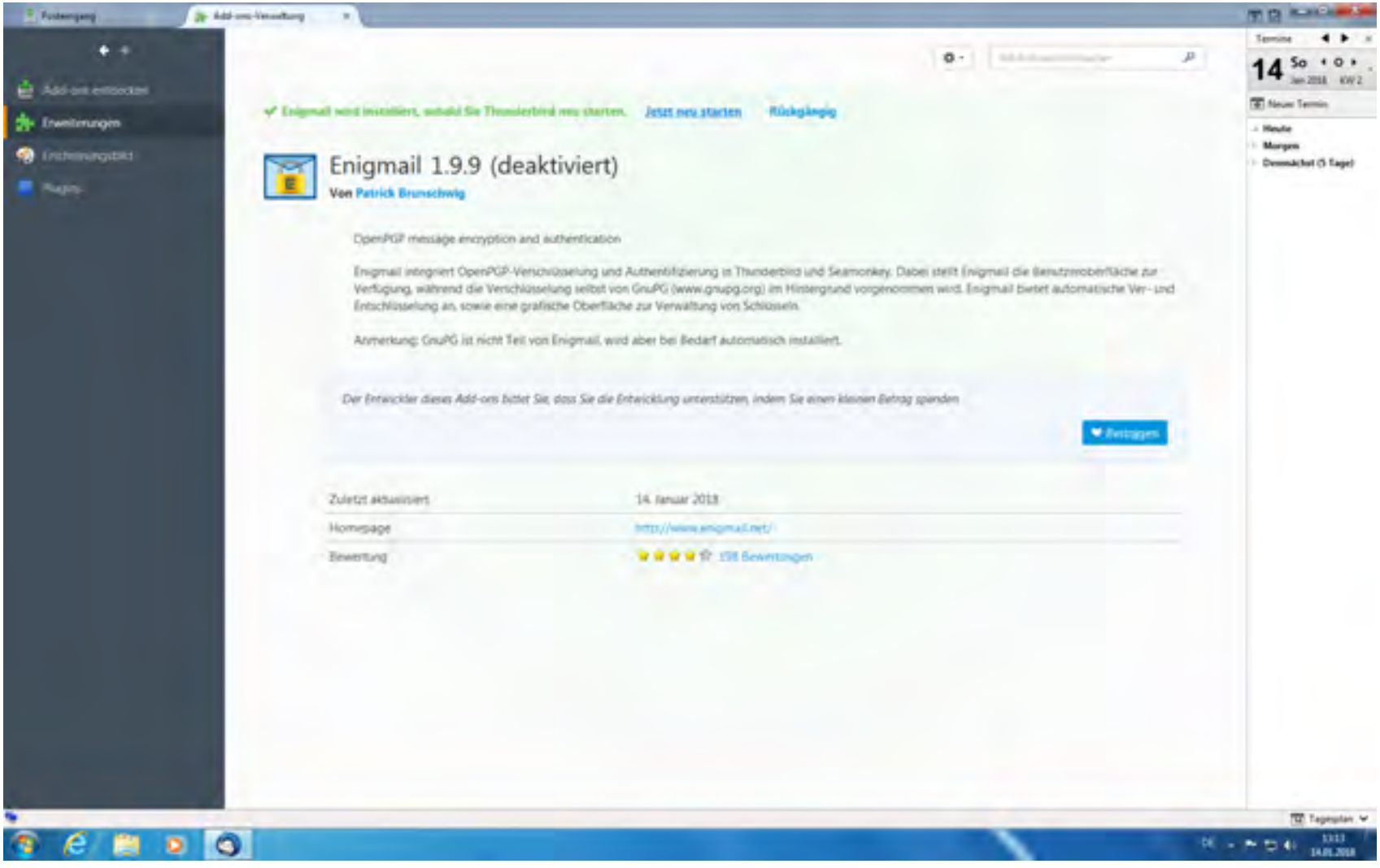
$$m = c^d mod(n)$$
$$m = 2^{47} mod(143) = 7$$

cool.

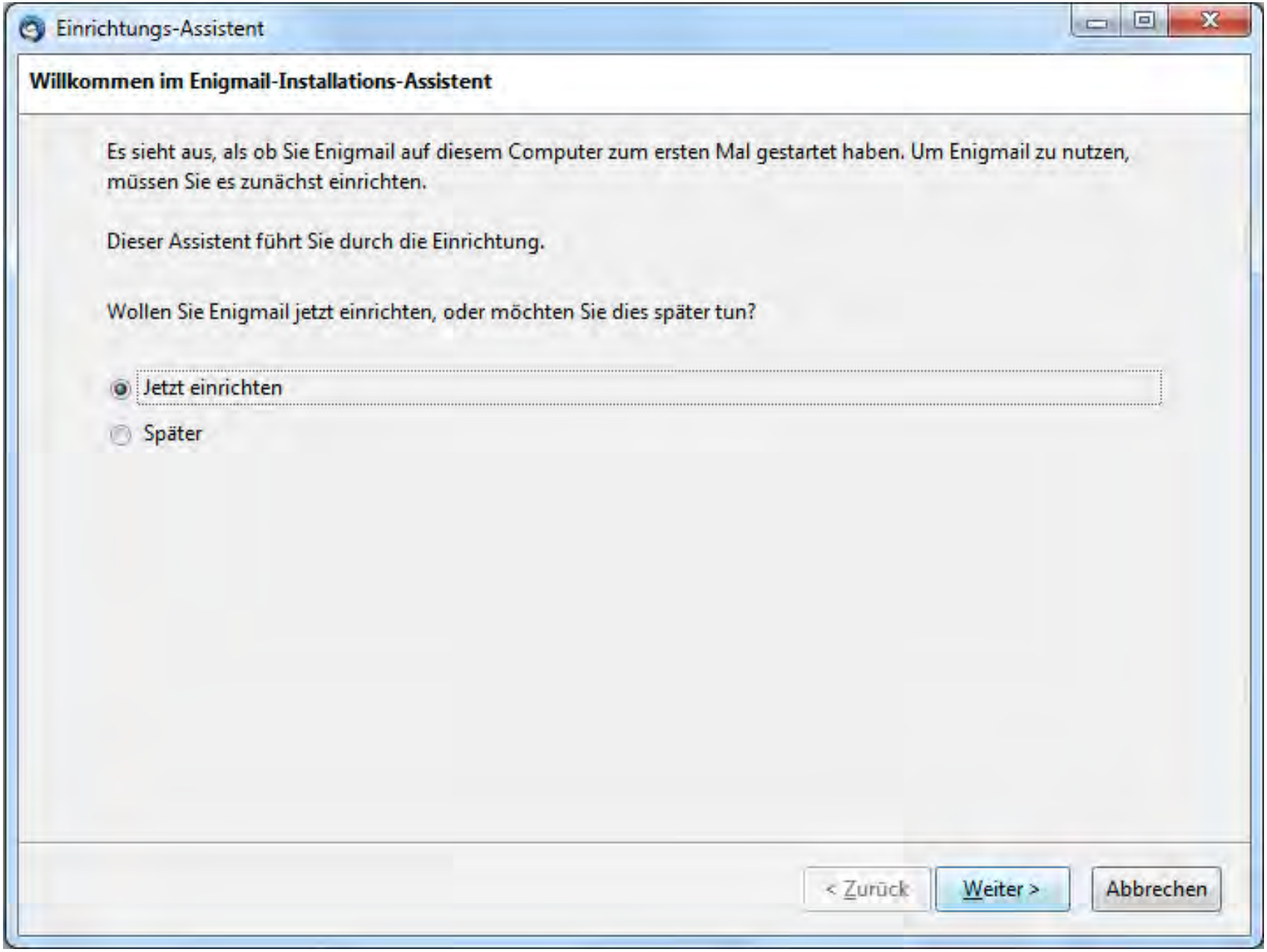
Einrichten von ENIGMAIL in Thunderbird



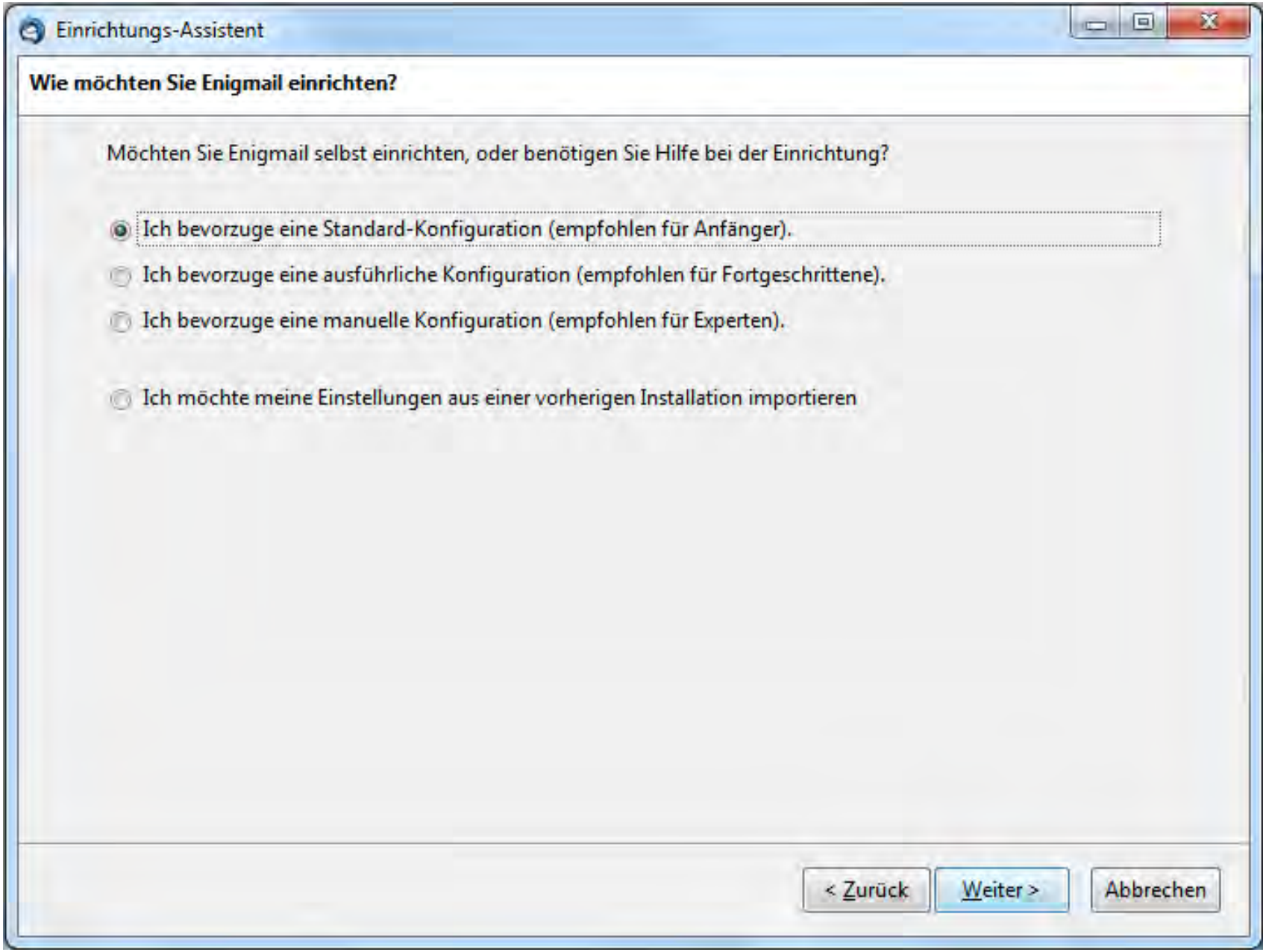
Einrichten von ENIGMAIL in Thunderbird



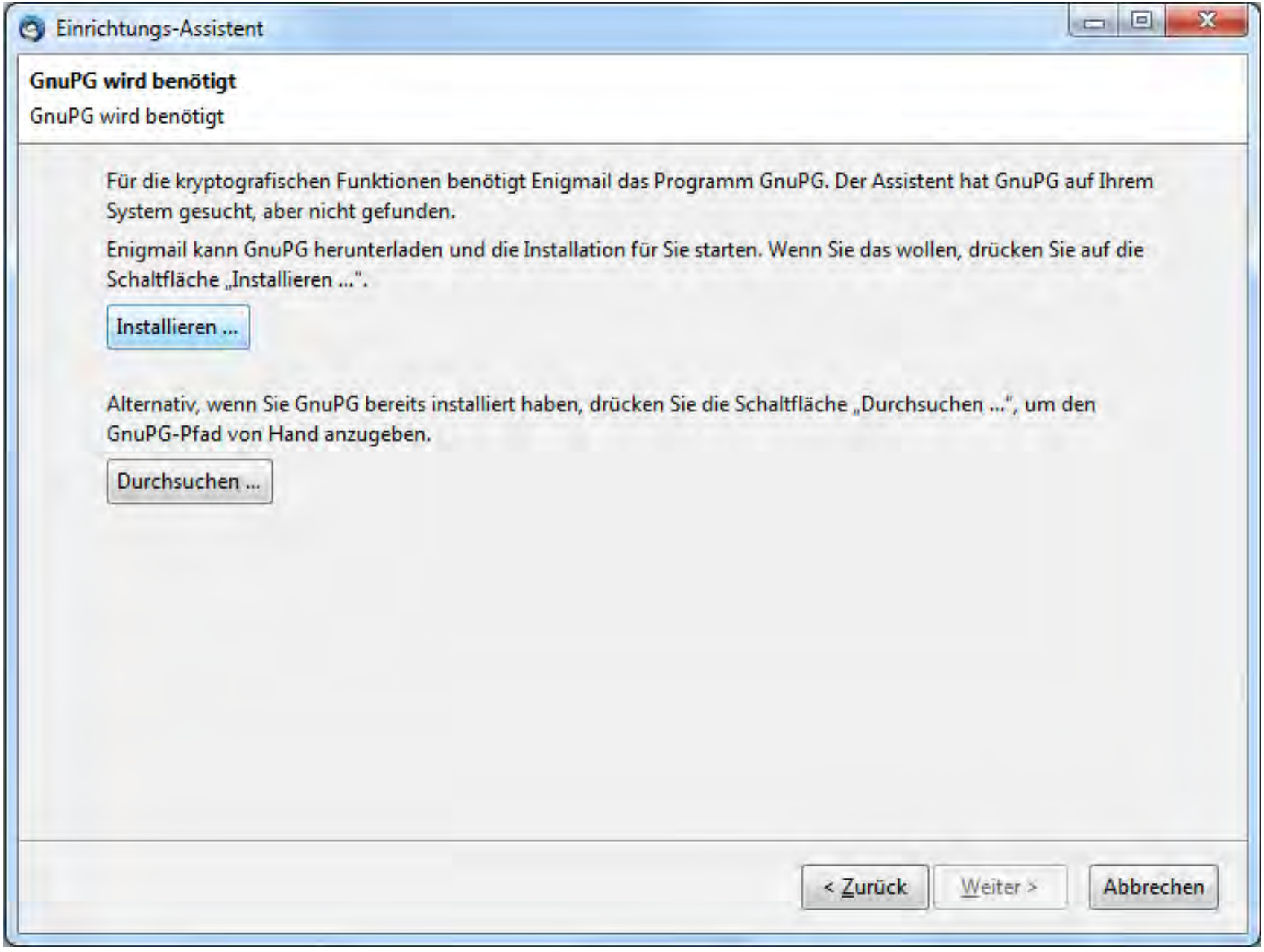
Einrichten von ENIGMAIL in Thunderbird



Einrichten von ENIGMAIL in Thunderbird

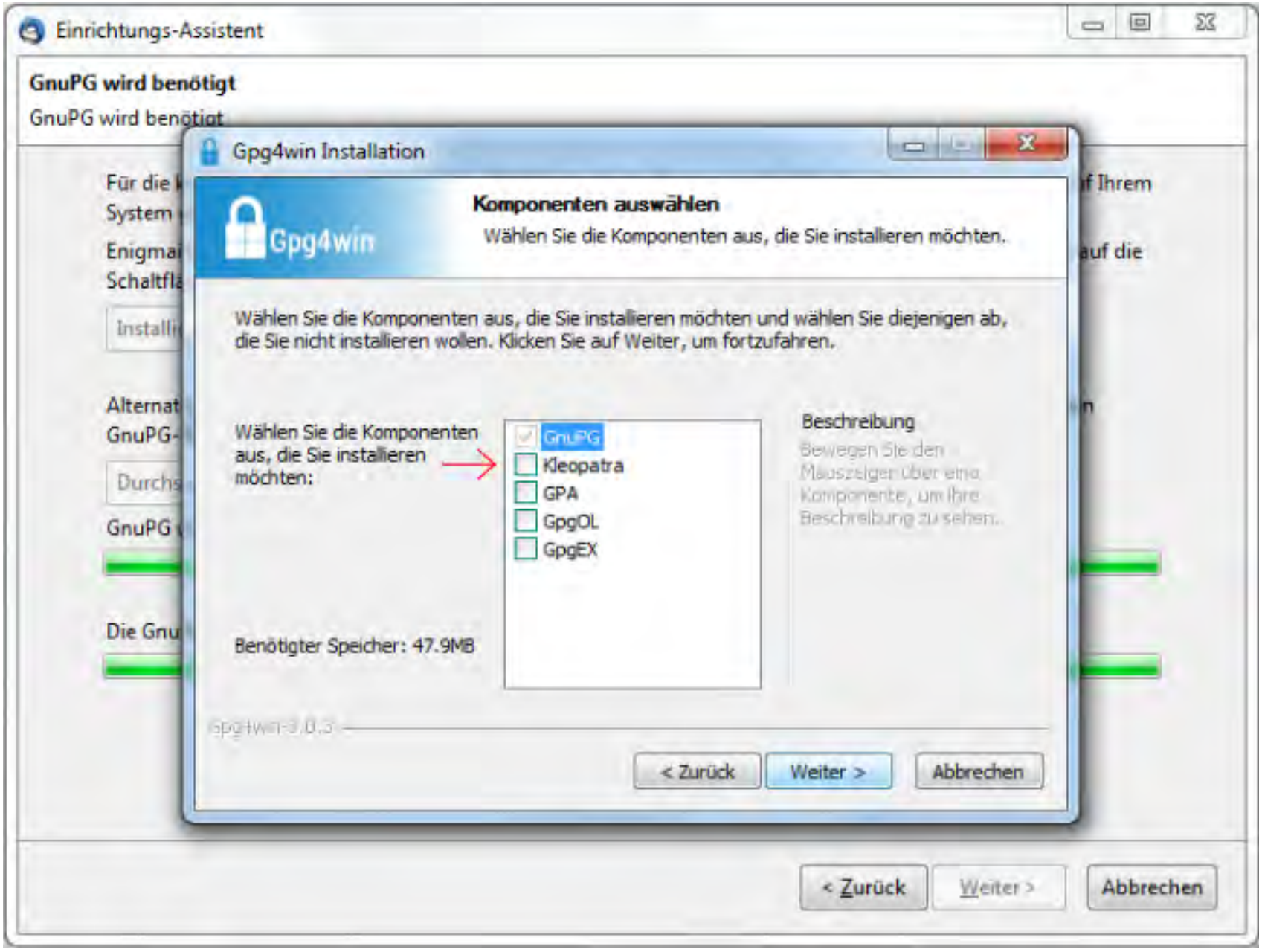


Einrichten von ENIGMAIL in Thunderbird

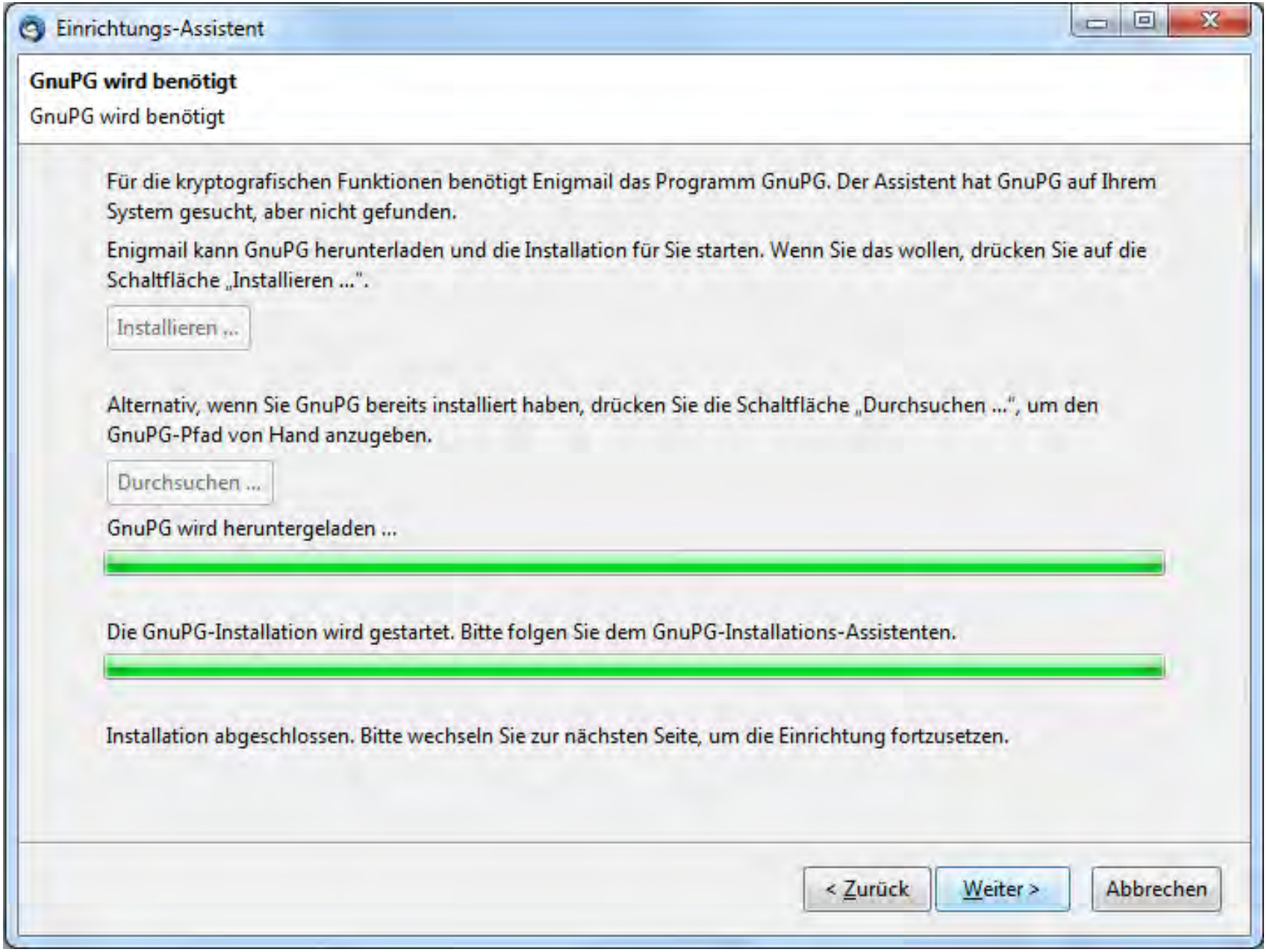


Einrichten von ENIGMAIL in Thunderbird

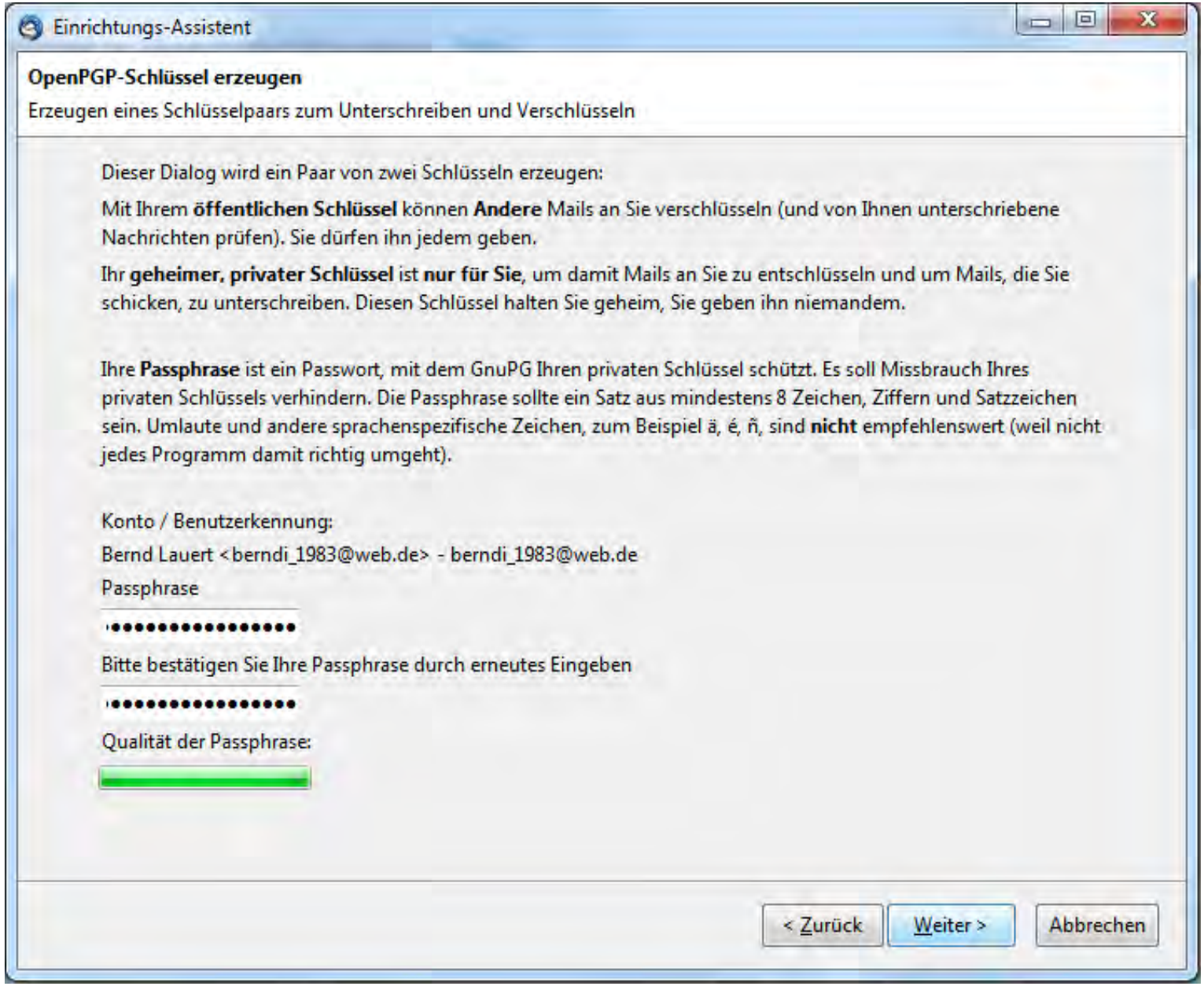
Einrichten von ENIGMAIL in Thunderbird



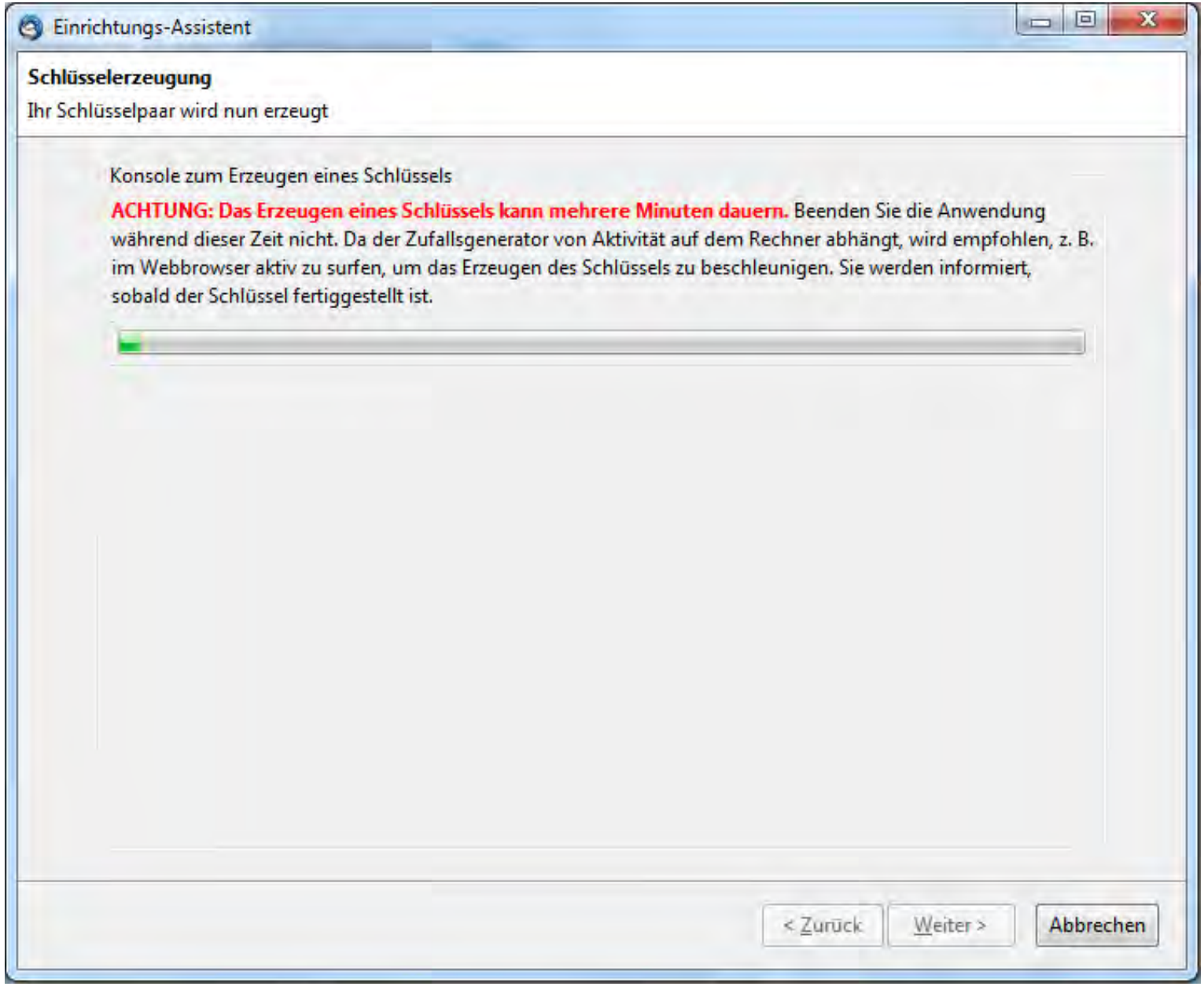
Einrichten von ENIGMAIL in Thunderbird



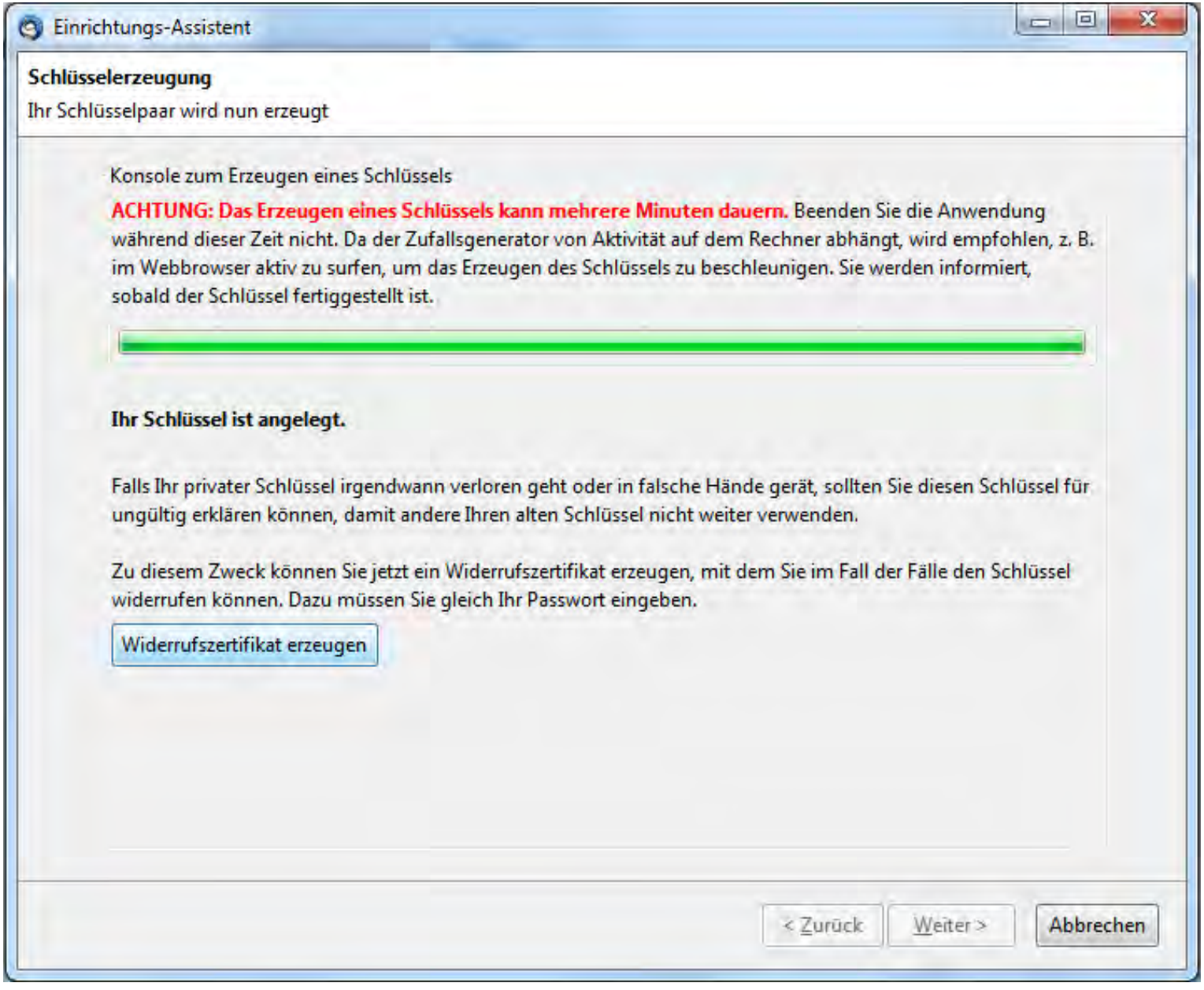
Einrichten von ENIGMAIL in Thunderbird



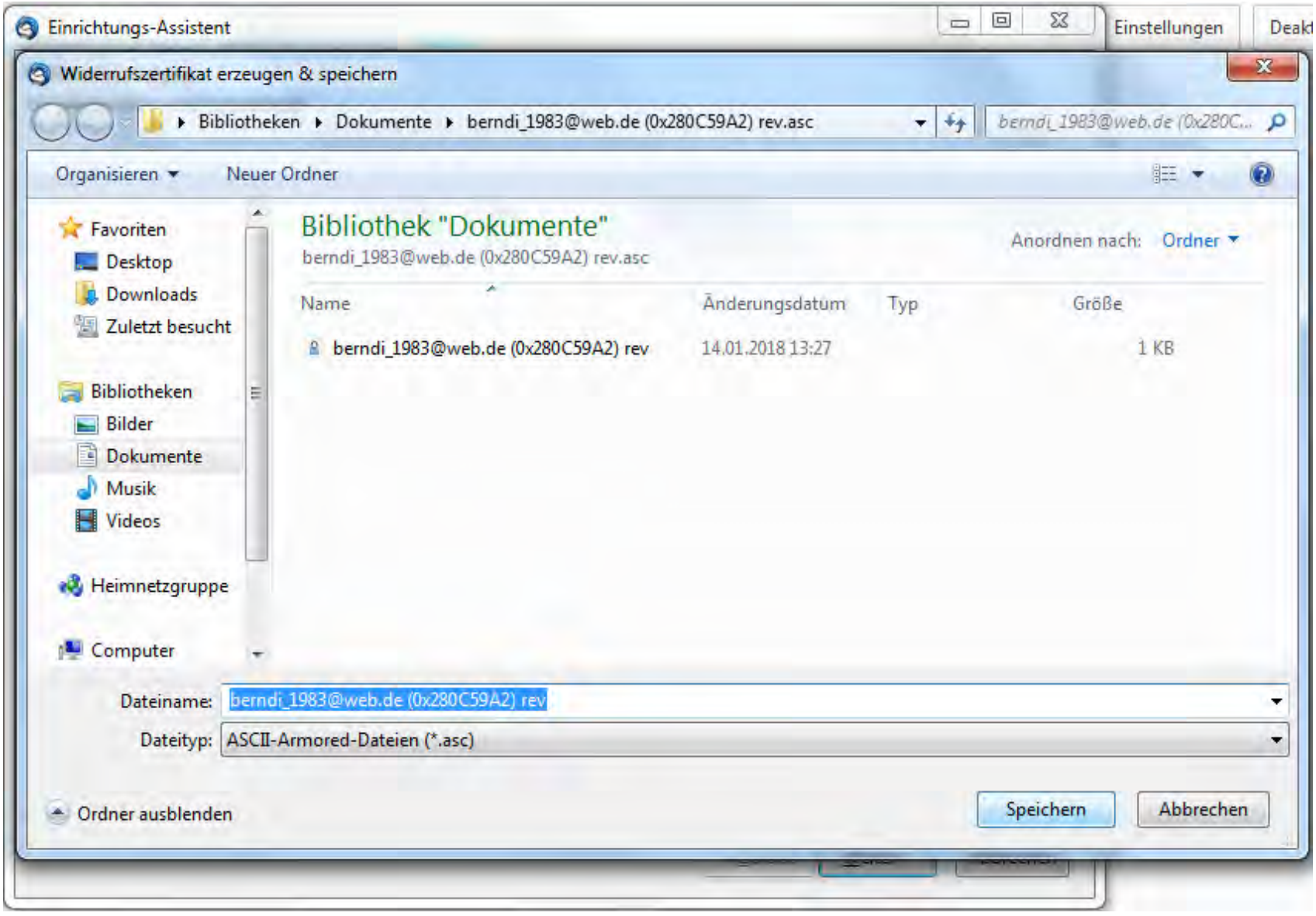
Einrichten von ENIGMAIL in Thunderbird



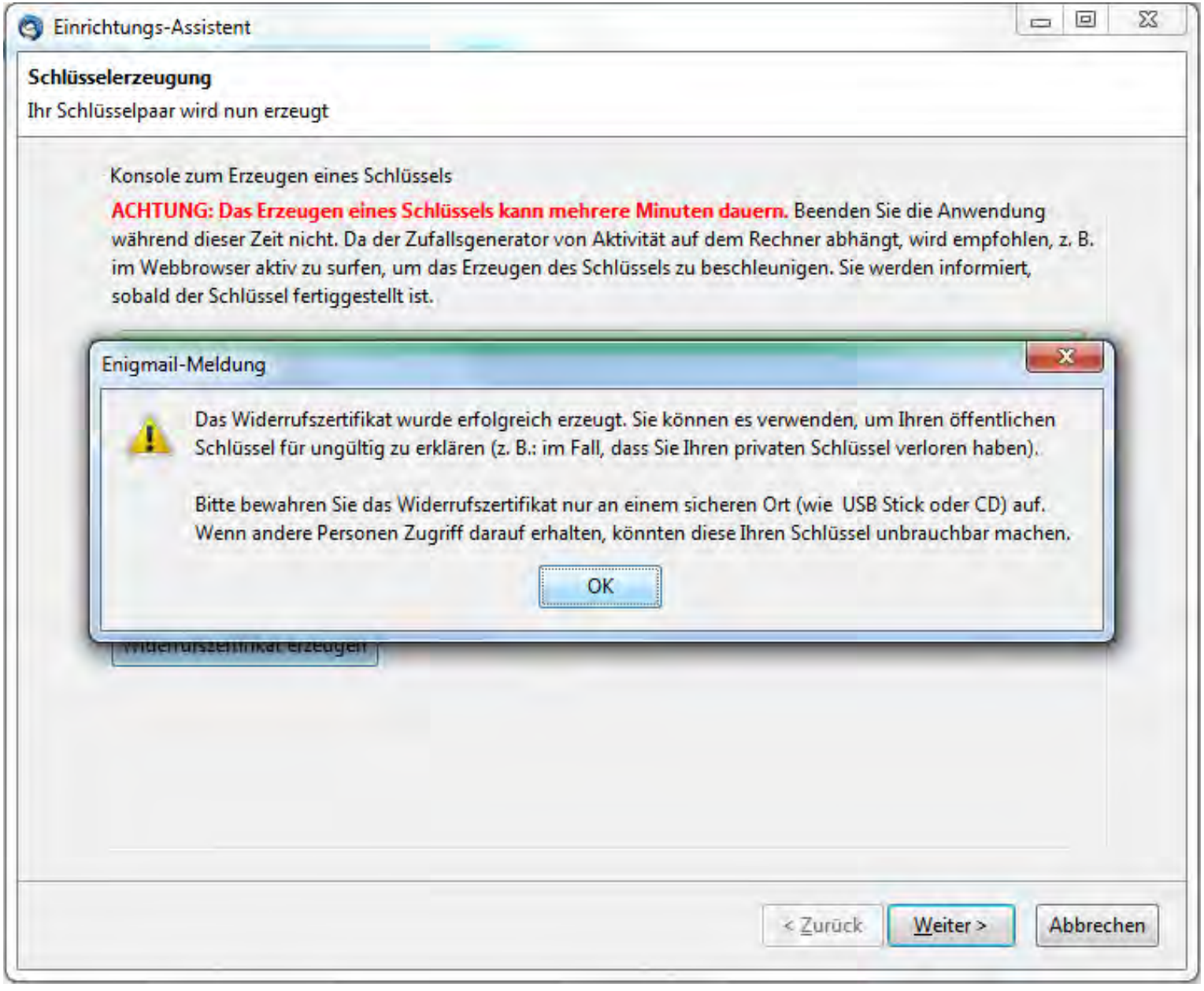
Einrichten von ENIGMAIL in Thunderbird



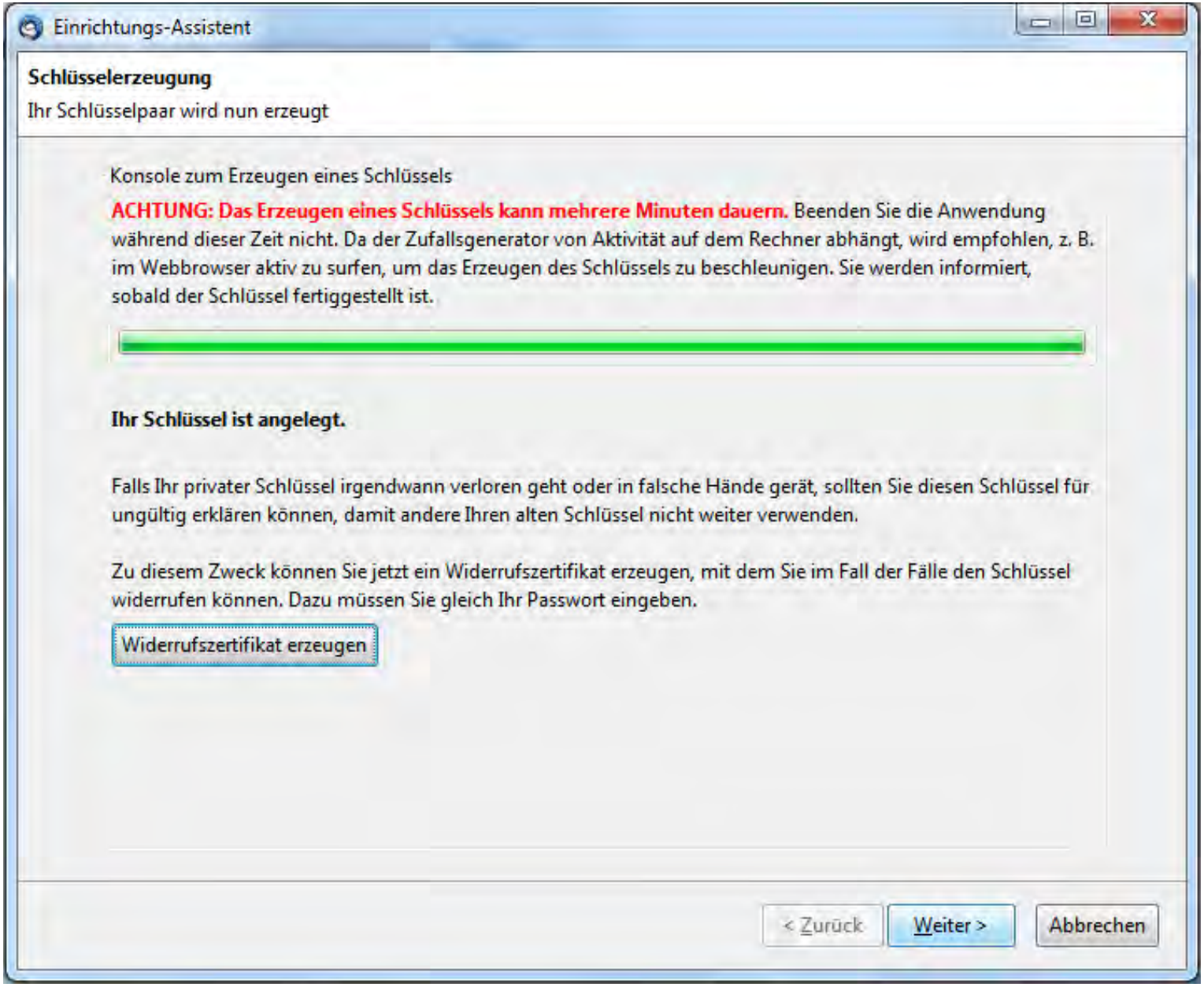
Einrichten von ENIGMAIL in Thunderbird



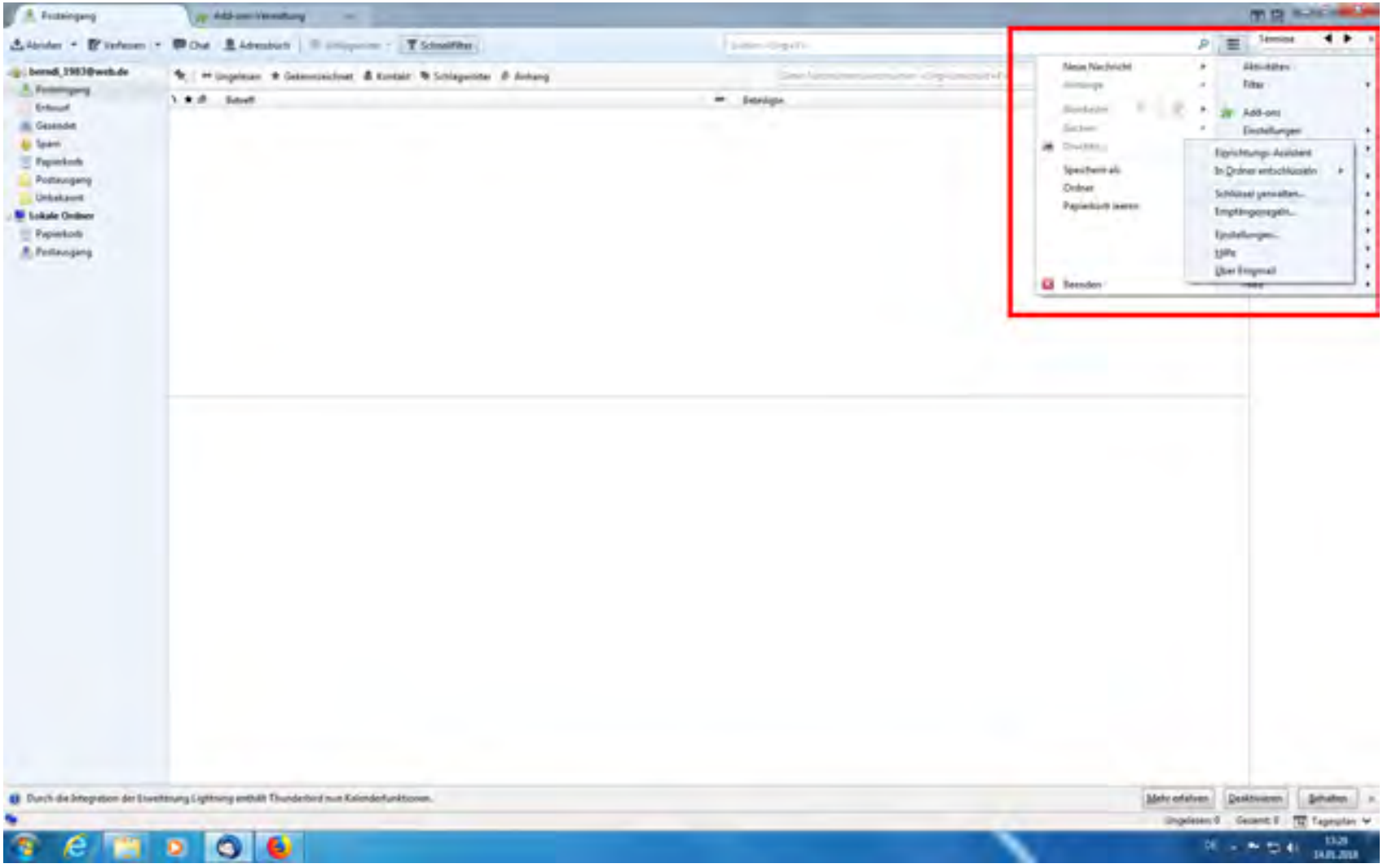
Einrichten von ENIGMAIL in Thunderbird



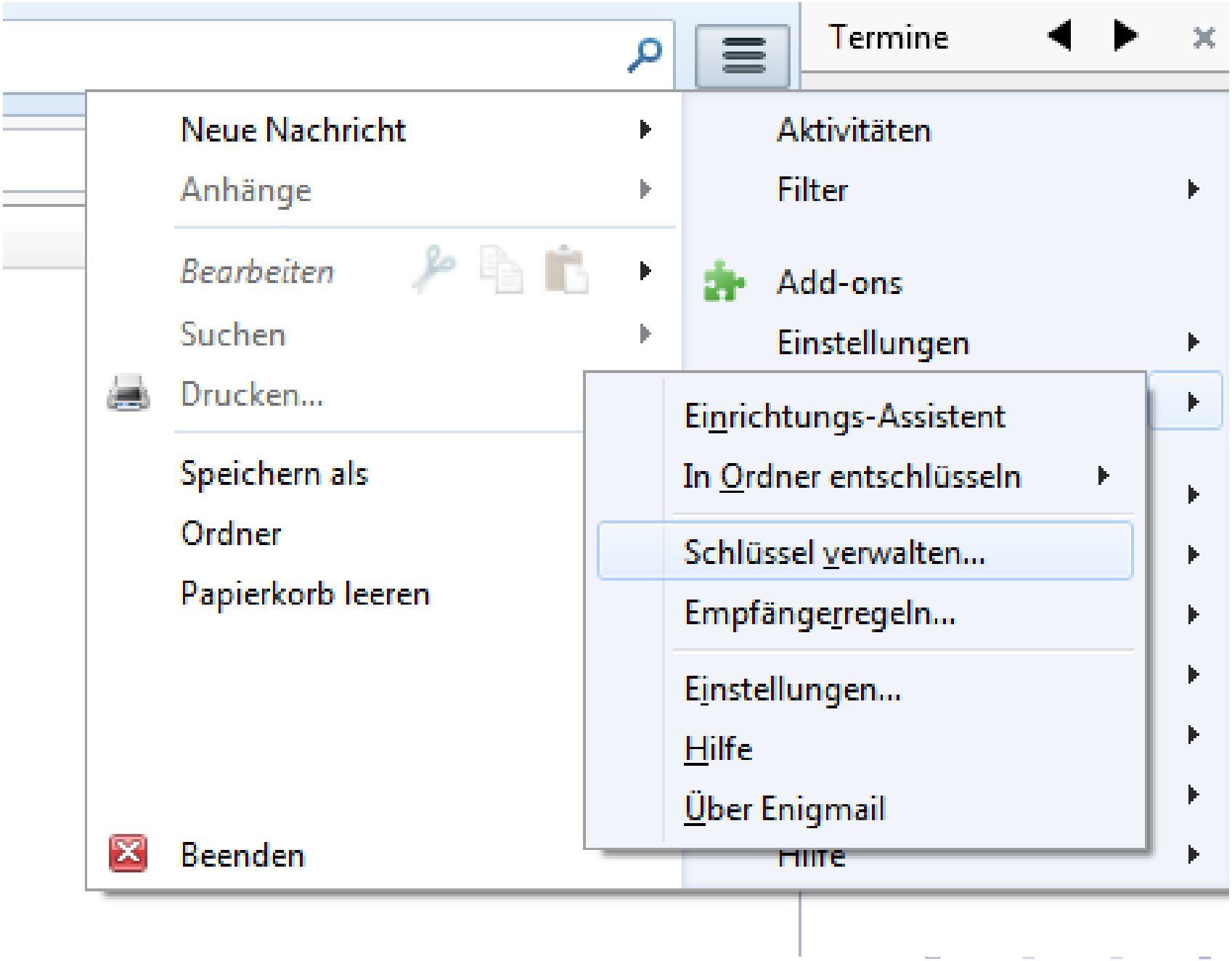
Einrichten von ENIGMAIL in Thunderbird



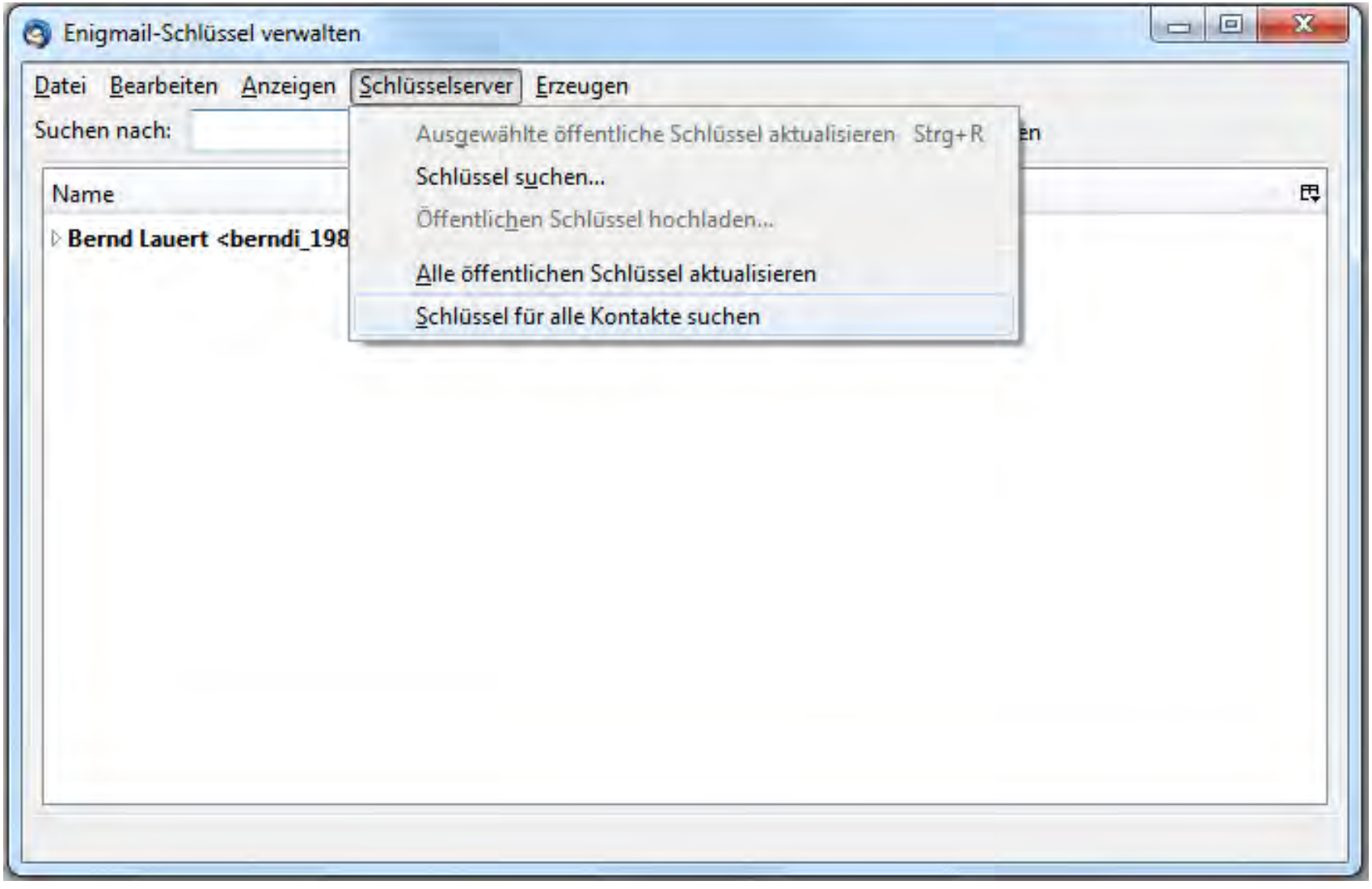
Einrichten von ENIGMAIL in Thunderbird



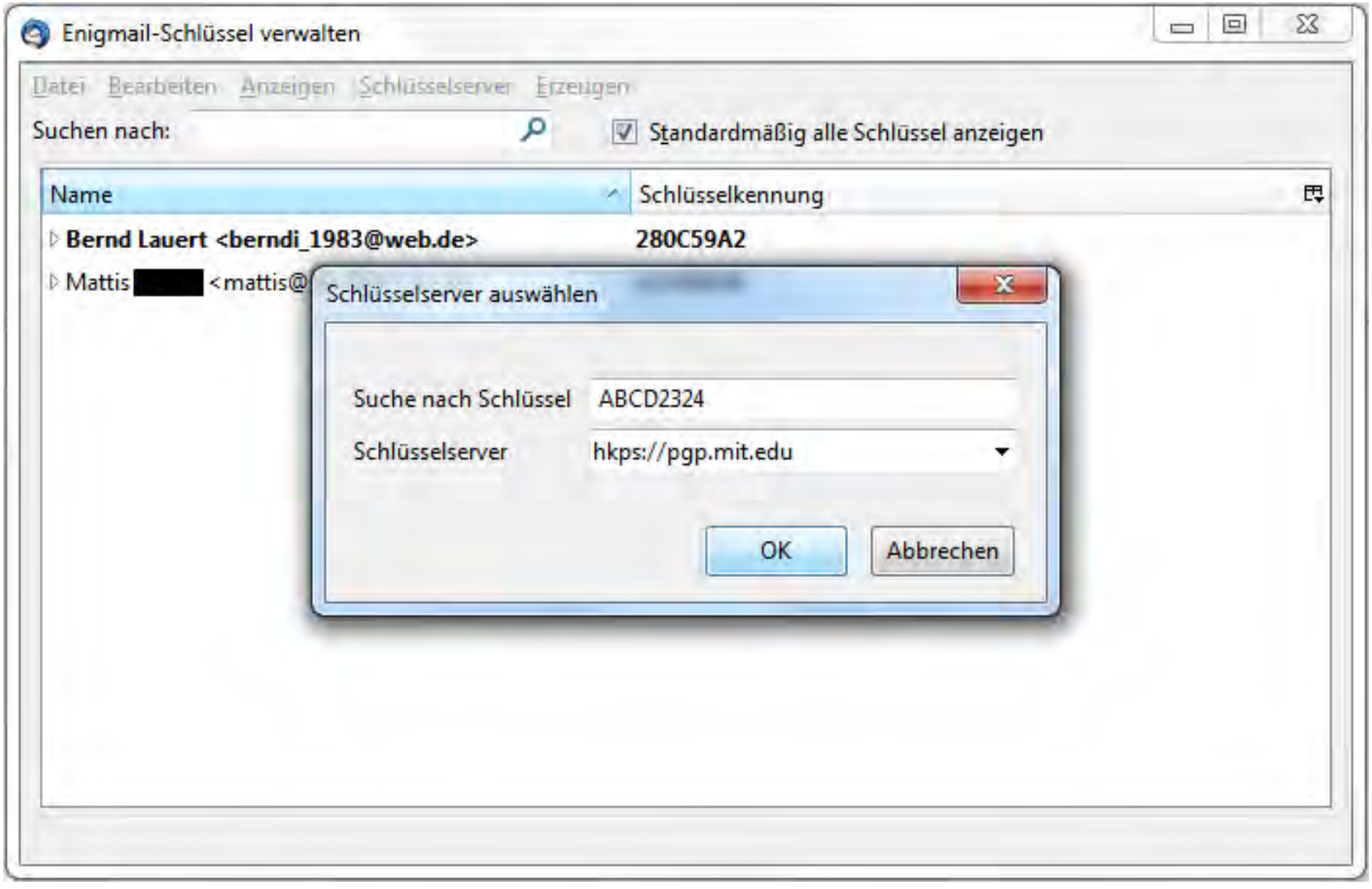
Einrichten von ENIGMAIL in Thunderbird



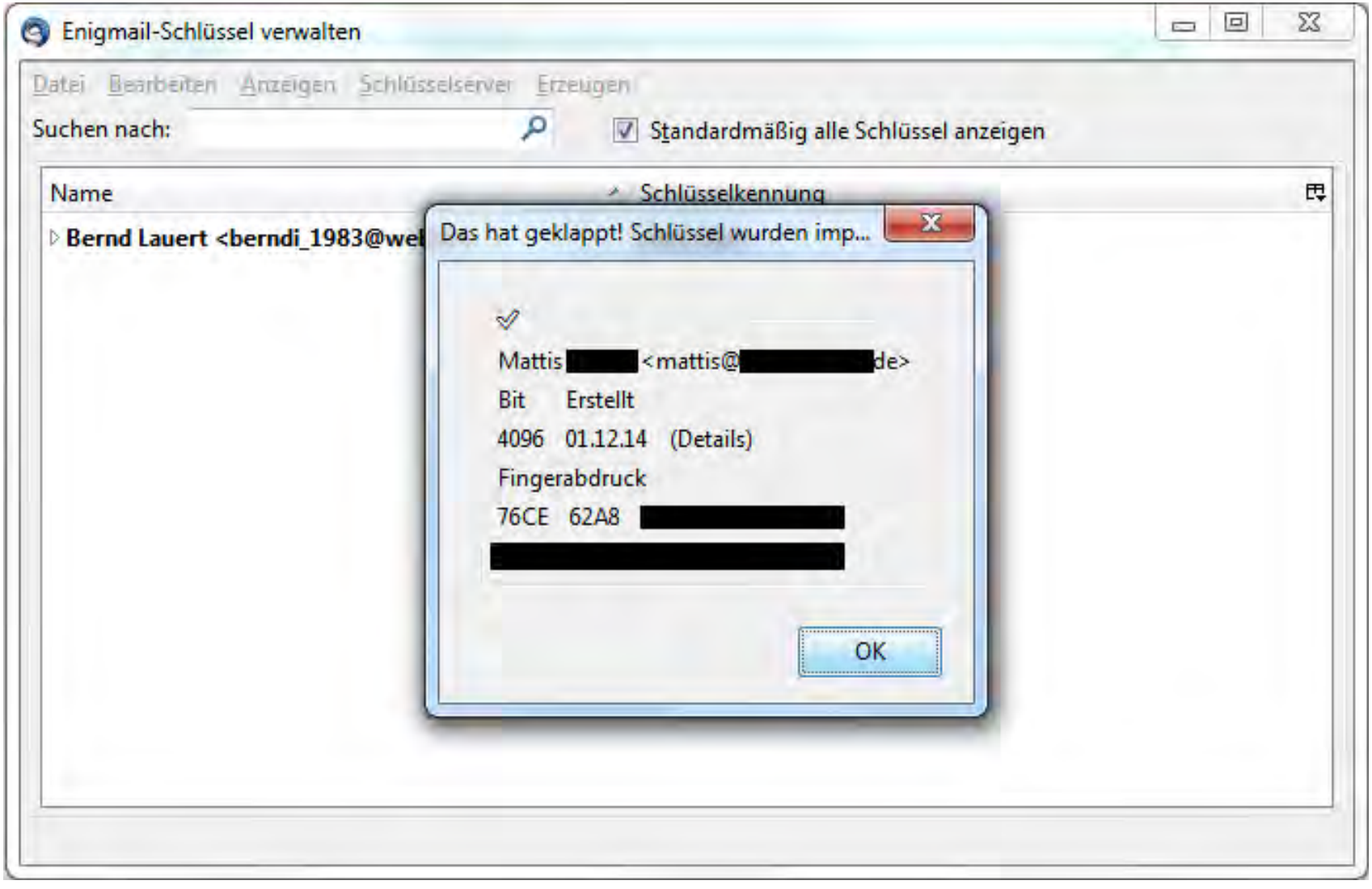
Hinzufügen eines Schlüssels mit ENIGMAIL in Thunderbird



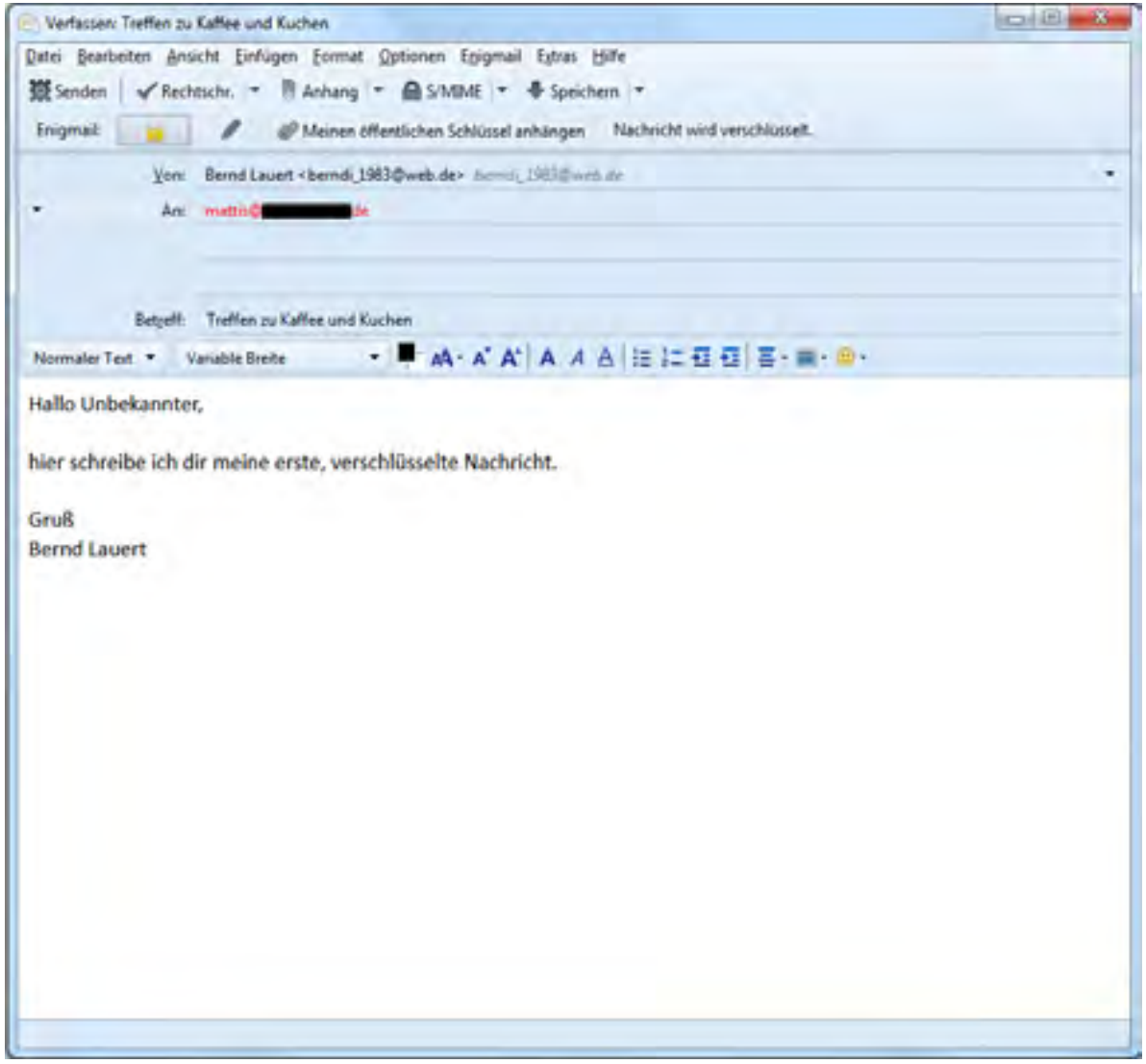
Hinzufügen eines Schlüssels mit ENIGMAIL in Thunderbird



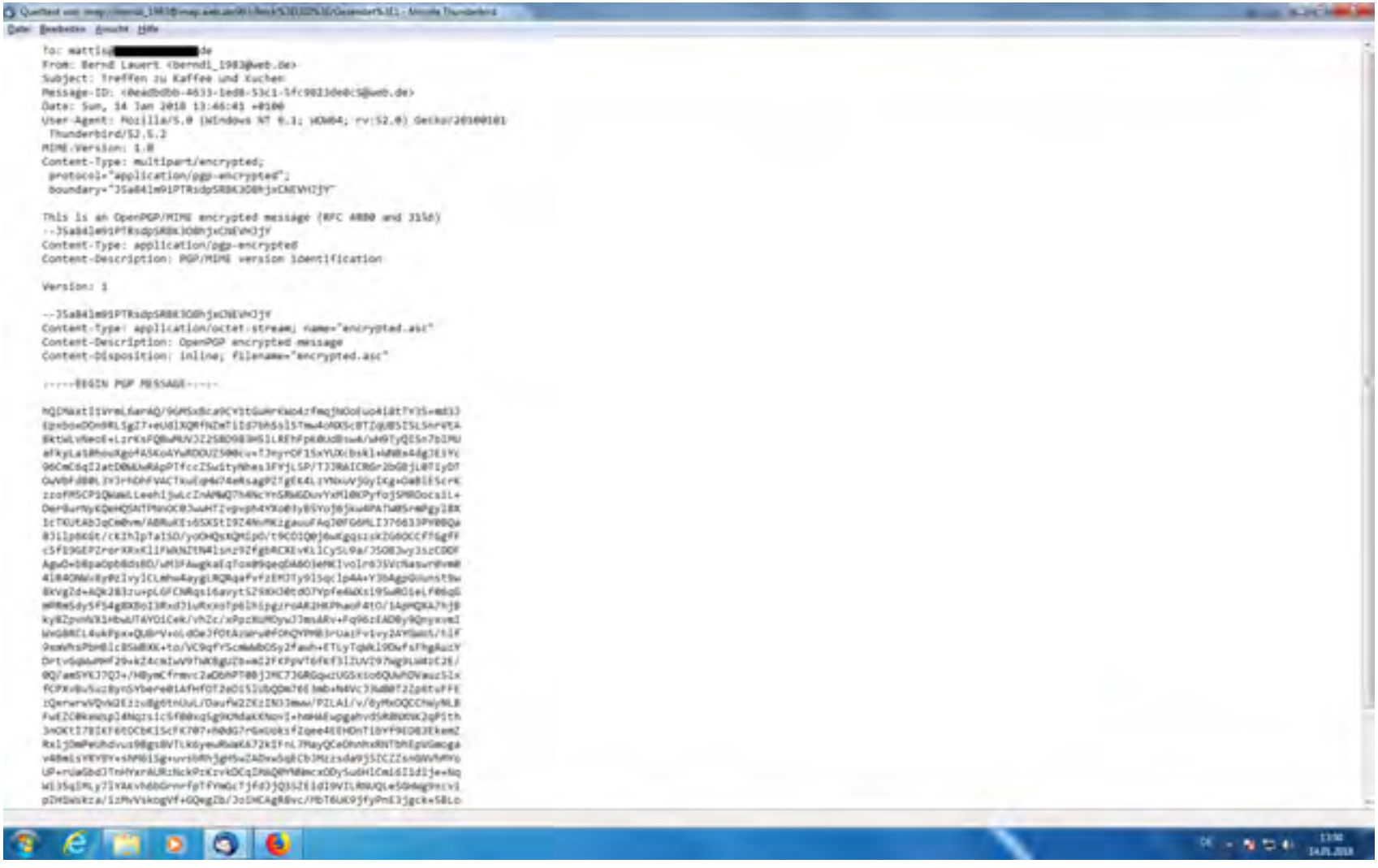
Hinzufügen eines Schlüssels mit ENIGMAIL in Thunderbird



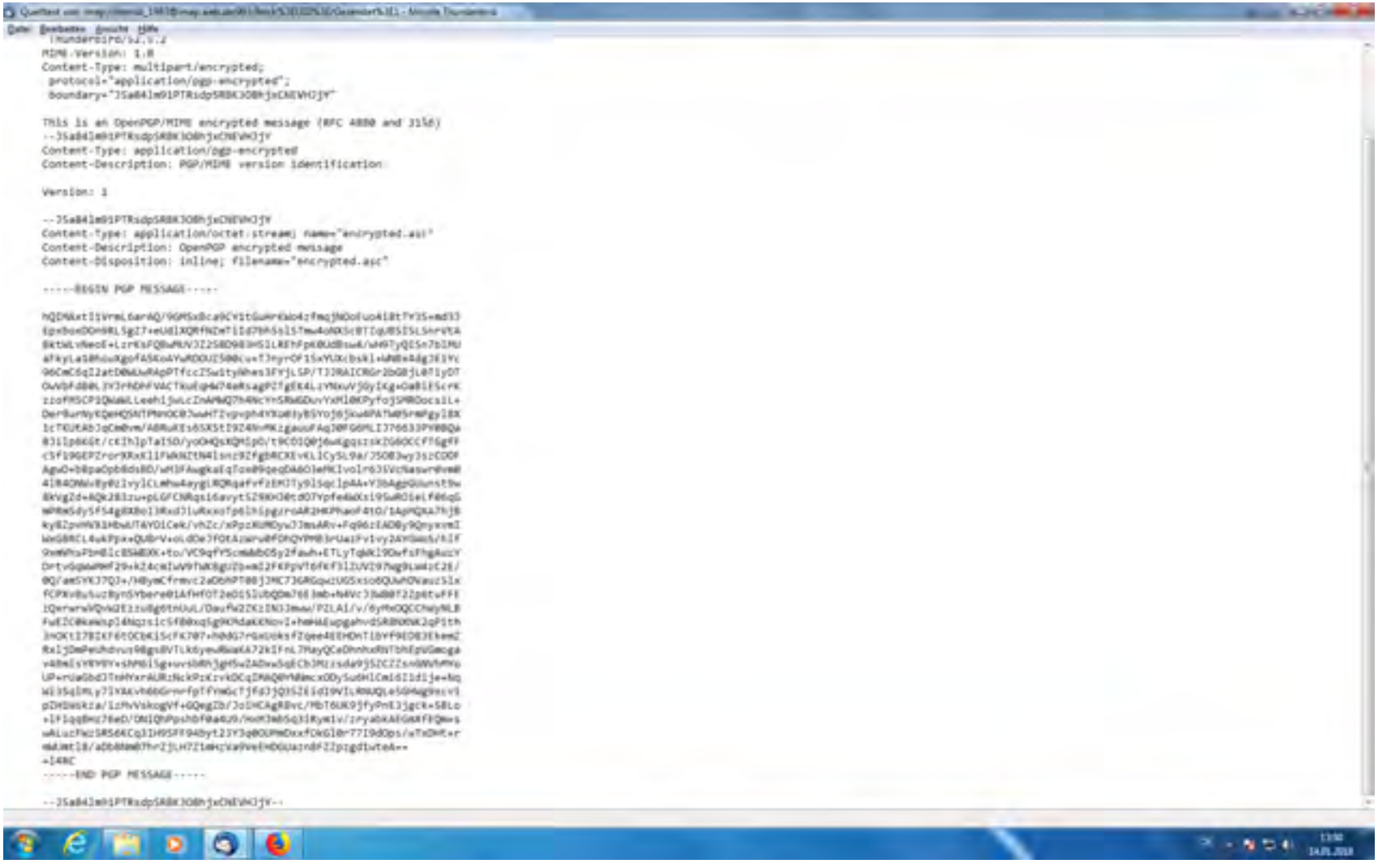
Schreiben einer verschlüsselten Nachricht mit ENIGMAIL in Thunderbird



Quelltext einer verschlüsselten Nachricht



Quelltext einer verschlüsselten Nachricht



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)
- (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 knackat doch eh alles

- Supercomputer schaffen etwa 100.000 Passwörter pro Sekunde

Bonusfolie 2 : Die NSA knackat doch eh alles

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

Bonusfolie 2 : Die NSA knackat doch eh alles

- Supercomputer schaffen etwa 100.000 Passwörter pro Sekunde
- Das Jahr hat 31556736 Sekunden.
- Annahme: Das Passwort besteht aus Groß- und Kleinbuchsabten, 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 $23 \cdot d \bmod 120 = 1$ -> $d = 47$

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.