

E-Mails verschlüsseln

Die folgende Anleitung zeigt dir, wie du deine E-Mails verschlüsseln kannst. Hierfür brauchst du natürlich eine E-Mailadresse. Sollte es der Fall sein, dass du bisher keine hast, oder das sicherhaltshalber noch nicht mit deiner eigenen E-Mailadresse testen möchtest, kannst du eine von deiner Lehrerin bzw. deinem Lehrer bereitgestellte E-Mailadresse benutzen.

Schritt 1 – Installation von Thunderbird

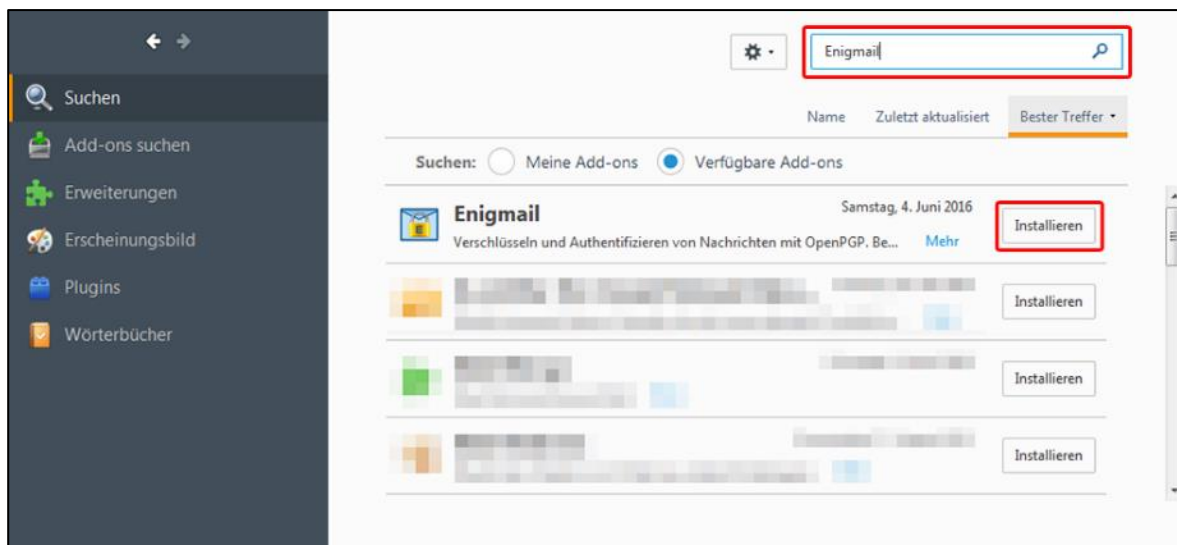
Als E-Mailprogramm verwenden wir Thunderbird. Sollte das Programm noch nicht auf dem Computer installiert sein, dann findest du unter folgender URL die Installationsdatei:

<https://www.mozilla.org/de/thunderbird/>

Anschließend solltest du das Programm installieren und einen E-Mailaccount einrichten.

Schritt 2 – Installation von Enigmail

Standardmäßig bietet Thunderbird nicht die Möglichkeit E-Mails zu verschlüsseln. Daher benötigen wir das Add-on *Enigmail*. Klicke dazu in der Menüleiste auf den Reiter *Extras* und wähle *Add-ons*. (Sollte die Menüleiste nicht sichtbar sein, musst du die *ALT*-Taste drücken.) Anschließend gibst du in das Suchfeld *Enigmail* ein und kannst das Add-on *installieren*.



Schritt 3 – GnuPG installieren

Nach dem das Add-on installiert wurde, kannst du Thunderbird erst einmal schließen (es sollte ein Neustart des Programms notwendig sein). Anschließend benötigen wir noch PGP bzw. die Implementierung GnuPG. Auf der offiziellen Webseite zu GnuPG solltest du ein entsprechendes Programm samt Download für dein Betriebssystem finden (ganz unten auf der Seite unter *GnuPG binary releases*):

<https://www.gnupg.org/download/index.html>

Für Windows kannst du auf Gpg4win klicken und die aktuellste Version herunterladen. Anschließend musst du das Programm noch installieren.



Schritt 3 – Enigmail einrichten

Nach der Installation des Add-ons ist es notwendig, dass du Thunderbird neu startest. Nach dem Neustart öffnet sich ein Fenster mit dem Einrichtungs-Assistenten von Enigmail. Sollte das Fenster nicht erscheinen, so kannst du es unter dem Menüpunkt *Enigmail* > *Einrichtungs-Assistent* aufrufen. Folge anschließend den folgenden Anweisungen.

Willkommen im Enigmail-Installations-Assistent

Es sieht aus, als ob Sie Enigmail auf diesem Computer zum ersten Mal gestartet haben. Um Enigmail zu nutzen, müssen Sie es zunächst einrichten.

Dieser Assistent führt Sie durch die Einrichtung.

Wollen Sie Enigmail jetzt einrichten, oder möchten Sie dies später tun?

☒ Jetzt einrichten
☐ Später

Wähle *Jetzt einrichten* aus und klicke auf *Weiter >*. Anschließend kannst du auswählen, dass du die *Standard-Konfiguration bevorzugst* und dann auf *Weiter >* klicken. Sollte dir im nächsten Schritt angezeigt werden, dass GnuPG (eine Umsetzung von PGP) benötigt, dann wähle den entsprechenden Pfad zu GnuPG aus und klicke auf *Weiter >*. Nun solltest du die Aufforderung erhalten, einen OpenPGP-Schlüssel zu erzeugen.

OpenPGP-Schlüssel erzeugen
Erzeugen eines Schlüssels zum Unterschreiben und Verschlüsseln

Dieser Dialog wird ein Paar von zwei Schlüsseln erzeugen:
 Mit Ihrem **öffentlichen Schlüssel** können **Andere** Mails an Sie verschlüsseln (und von Ihnen unterschriebene Nachrichten prüfen). Sie dürfen ihn jedem geben.
 Ihr **geheimer, privater Schlüssel** ist **nur für Sie**, um damit Mails an Sie zu entschlüsseln und um Mails, die Sie schicken, zu unterschreiben. Diesen Schlüssel halten Sie geheim, Sie geben ihn niemandem.

Ihre **Passphrase** ist ein Passwort, mit dem GnuPG Ihren privaten Schlüssel schützt. Es soll Missbrauch Ihres privaten Schlüssels verhindern. Die Passphrase sollte ein Satz aus mindestens 8 Zeichen, Ziffern und Satzzeichen sein. Umlaute und andere sprachenspezifische Zeichen, zum Beispiel ä, é, ñ, sind **nicht** empfehlenswert (weil nicht jedes Programm damit richtig umgeht).

Konto / Benutzerkennung:

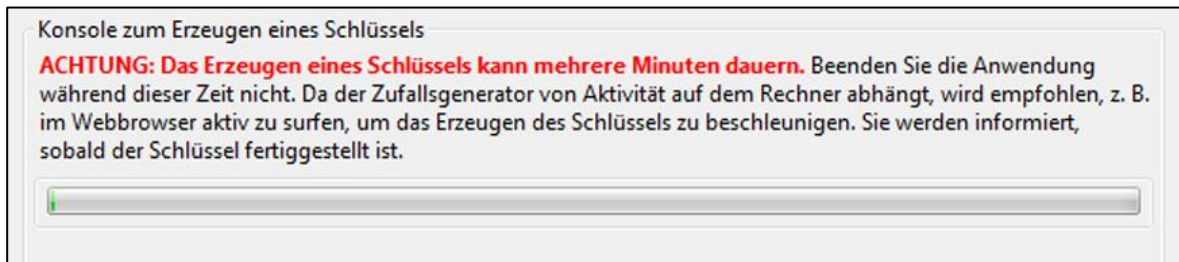
Passphrase

 Bitte bestätigen Sie Ihre Passphrase durch erneutes Eingeben

 Qualität der Passphrase:

Um ein Schlüsselpaar zu erzeugen benötigt der Assistent eine Passphrase (ein Passwort). Achte darauf, dass es möglichst sicher ist, d. h. dass die Qualitätsleiste möglichst voll ist.

Sobald du auf Weiter > geklickt hast, sollte das Schlüsselpaar generiert werden. Dies kann einige Zeit benötigen.



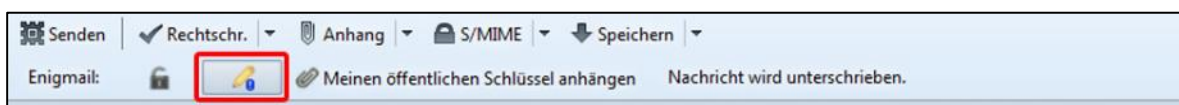
Speichere nun sicherheitshalber noch das Widerrufszertifikat ab. Dabei solltest du darauf achten, dass du es jetzt oder später an einen sicheren Ort ablegst. Das Widerrufszertifikat dient dazu, das soeben generierte Schlüsselpaar, dass nun mit deiner E-Mailadresse verknüpft ist, zu widerrufen. Mit einem Klick auf Weiter > ist die Einrichtung für deinen E-Mailaccount abgeschlossen.

Schritt 4 – Eine verschlüsselte E-Mail verschicken

Sobald du nun in Thunderbird eine E-Mail verschicken willst, hast du die Möglichkeit diese zu unterschreiben und/oder zu verschlüsseln.



Beachte, dass du zum Verschlüsseln einer Nachricht den öffentlichen Schlüssel des Empfängers benötigst. Solltest du diesen nicht besitzen, wirst du vor dem Versenden gefragt, welchen Schlüssel du verwenden willst. Es empfiehlt sich also, nach dem Erzeugen eines Schlüsselpaares den eigenen öffentlichen Schlüssel mit deinen Bekannten und Freunden auszutauschen. Beim unterschreiben einer E-Mail wird der öffentliche Schlüssel automatisch beigefügt, außerdem weiß der Empfänger so, dass du der Absender bist.



Versendest du eine verschlüsselte oder unterschriebene Nachricht, dann wirst du immer nach der dazugehörigen Passphrase gefragt.

