Tutorial: E-Mails verschlüsseln per Browser und Mailvelope

Ich habe ein neues Tutorial von der Website des Vereins German Privacy Fund kopiert und bitte das sachverständige Publikum zu kommentieren, zu berichtigen und auf Fehler hinzuweisen.

Lernziele:
– Installieren des Browser-Add-ons Mailvelope
– (einmaliges) Erzeugen eines Schlüsselpaares,
– Export und Import öffentlicher Schlüssel,
– Senden einer verschlüsselten E-Mail.
Dauer: ca. 30 Minuten

Zeitaufwand: fünf Minuten (und etwas Zeit zum Downloaden des Add-ons)
Schwierigkeitsgrad: leicht

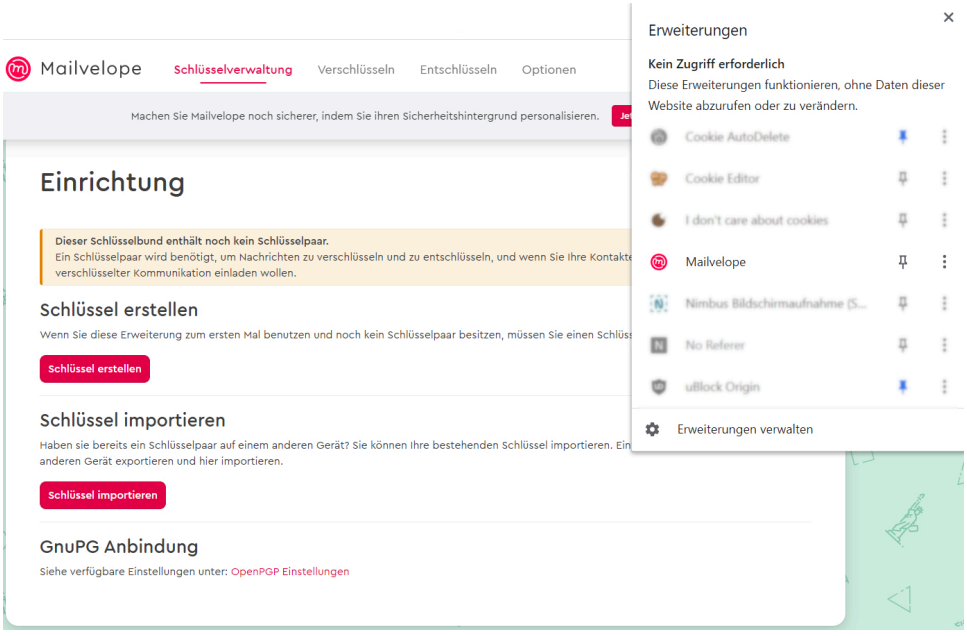
Installieren Sie das Browser-Add-on Mailvelope für Chrome (Windows) und Chromium (Linux) – Mailvelope für Firefox (Windows) und Firefox (Linux) – Mailvelope für Microsoft Edge (Windows) – Mailvelope für Opera.

Hinweise:
– Das Add-on funktioniert für alle Browser und Betriebssystem fast identisch.
– Mailvelope gibt es auf für das MacOS-Mail-Programm Mail , aber nur kombiniert mit GPGtools (das jedoch ist nicht gratis).
– Ihr Provider muss das Feature unterstützen, die meisten großen Provider tun das.
– Diejenigen, mit denen Sie verschlüsselt kommunizieren

wollen, müssen Mailvelope *nicht* benutzen, nur GnuPG oder E-Mail-Programme wie Thunderbird, die das Verschlüsselungsprogramm implementiert haben.
– Mailvelope funktioniert *nicht* bei Browsern mobiler Endgeräte.
– Die „häufig gestellte Fragen“ (FAQ) auf der Website von Mailvelope und das Tutorial sind hervorragend und selbsterklärend. Sie würden jedoch zwei Wochen brauchen, um alles zu lesen. Das Wichtige wird nicht vom weniger Wichtigen getrennt.

Vor- und Nachteile von Mailvelope

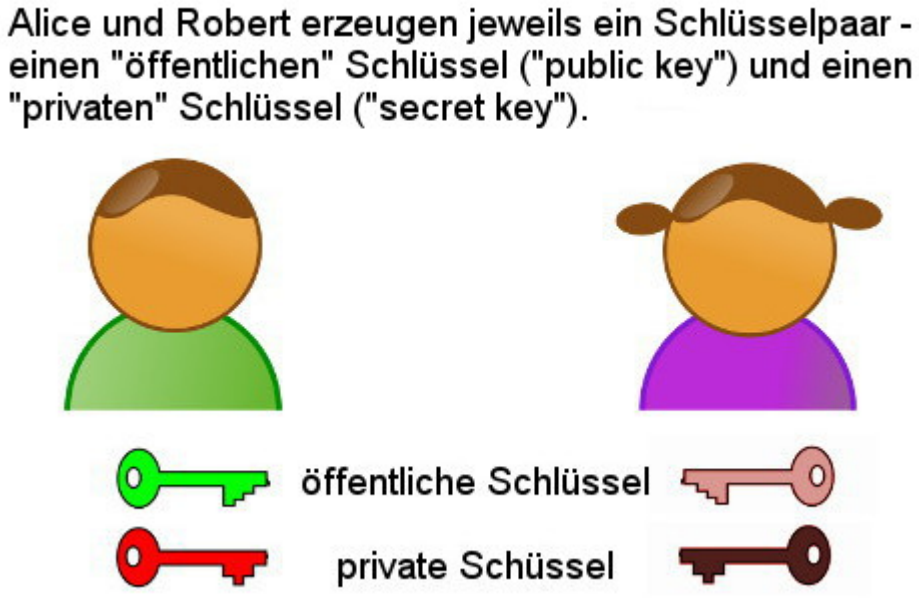
Sie sollten dieses Add-on nur benutzen, wenn Sie ihre E-Mails ausschließlich per Webmail, also mit dem Browser lesen. Sie müssen Mailvelope aber auf jedem der von Ihnen genutzten Browser installieren und auch Ihr Schlüsselbund dorthin kopieren – eine Alternative ist nur copy & paste eines schon verschlüsselten Textes in das geöffnete Webmail-Fenster. Das kann mühsam werden. Wenn Sie aber schon GnuPG und dessen Feature *Kleopatra* installiert haben, können Sie genau das (copy & paste) auch von dort aus tun und brauchten Mailvelope nicht.



Die Grafik anklicken, um sie zu vergrößern.

2. SCHRITT

Erzeugen eines Schlüsselpaares – eines *öffentlichen* und eines *privaten* Schlüssels.



5 MINUTEN

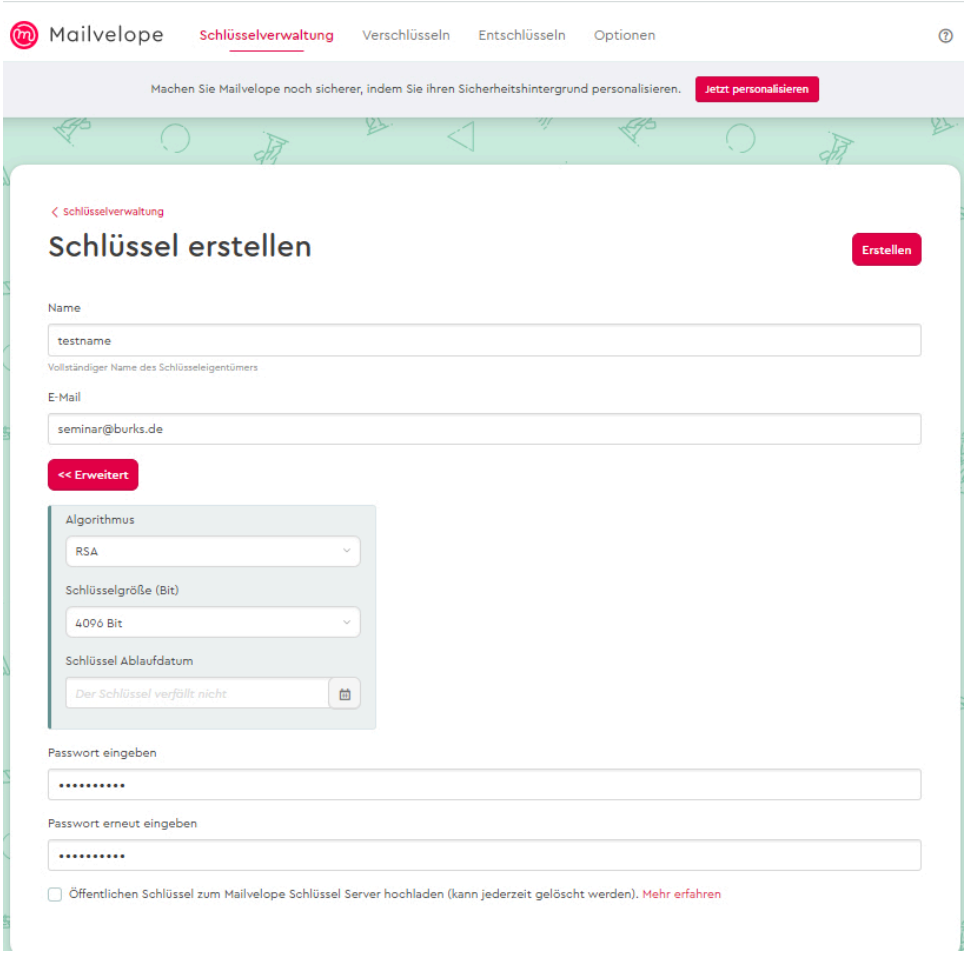
Zeitaufwand: fünf Minuten
Schwierigkeitsgrad: leicht

Nur Verschlüsselungssysteme, die mit einem öffentlichen Schlüssel („public key“) und einem privaten Schlüssel („private key“) arbeiten, sind sicher – so wie dieses.

Rufen Sie Mailvelope auf – es versteckt sich oben rechts in der Leiste, wo Sie vielleicht schon andere Add-ons installiert haben und sieht aus wie ein Klecks oder ein Blatt. Sie können alle Menüs bzw. Optionen des Add-ons Mailvelope vorerst ignorieren, außer Schlüssel verwalten“ und „Schlüsselbund“ (zwei Wörter für eine Opion).

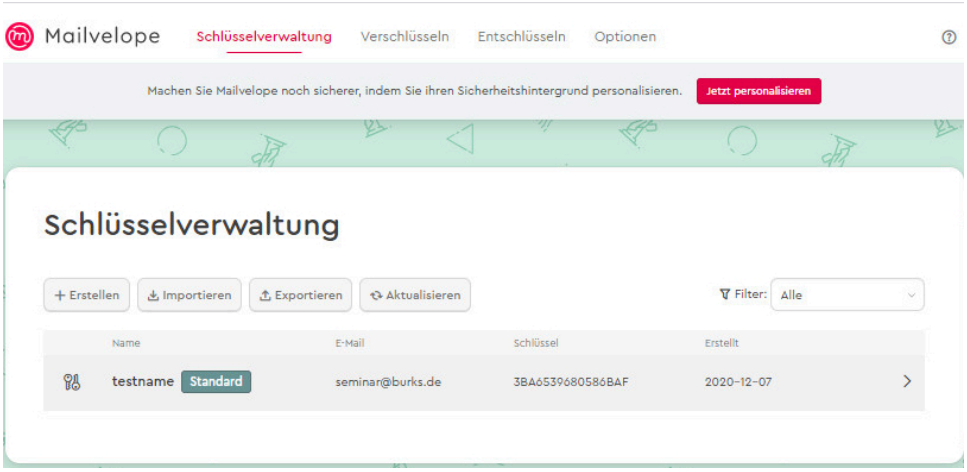
Sie *erstellen* jetzt ein Schlüsselpaar (oder importieren ein schon vorhandenes). Sie können auch einen Testschlüssel

erstellen, den sie später wieder löschen.



Die Grafik anklicken, um sie zu vergrößern.

Folgen Sie den Anweisungen, die sind auch für Laien verständlich. Es sind auch Schlüssel ohne Passwort möglich, wir empfehlen das nicht.

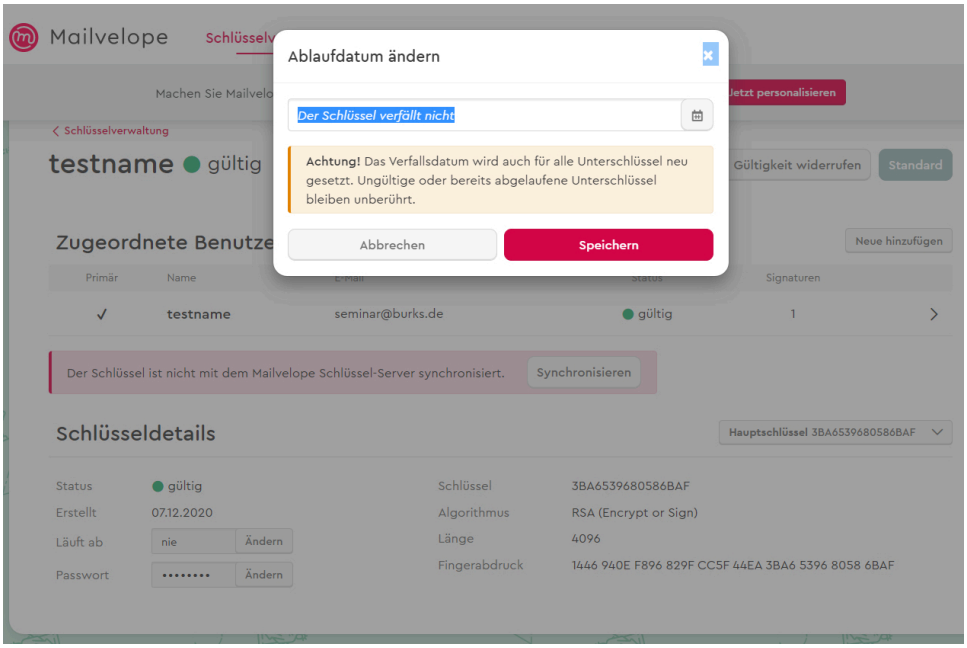


Die Grafik anklicken, um sie zu vergrößern.

Sie müssen jetzt nicht (wenn überhaupt) mit dem

Schlüsselserver von Mailvelope synchronisieren. Dieses Feature werden Sie vermutlich nie benötigen.

Im Beispiel oben haben wir einen Schlüssel „testname“ mit der E-Mail-Adresse seminar@burks.de erzeugt. In der Grafik unten sehen Sie dessen Eigenschaften, zum Beispiel den „Fingerprint“, eine Art unveränderliche „Quersumme“.



3. SCHRITT

Exportieren des eigenen öffentlichen Schlüssels – Importieren „fremder“ öffentlicher Schlüssel

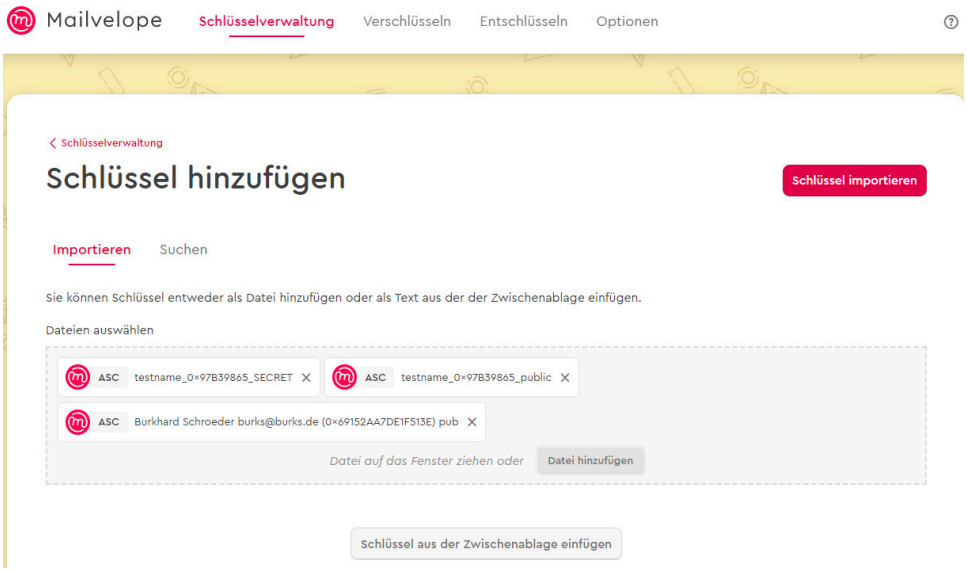
5 MINUTEN

Zeitaufwand: fünf Minuten

Schwierigkeitsgrad: leicht

Um starten zu können, müssen Sie jetzt den *öffentlichen* Schlüssel derjenigen Person, mit der sie verschlüsselte E-Mails tauschen wollen, *importieren* sowie Ihren eigenen *exportieren* und den offen verschicken. Den Fehler, den *geheimen* Schlüssel zu exportieren und zu versenden, können Sie nicht machen, weil Mailvelope davor warnt. (Das Feature

brauchen Sie nur für eine Sicherheitskopie Ihres Schlüsselpaares.)

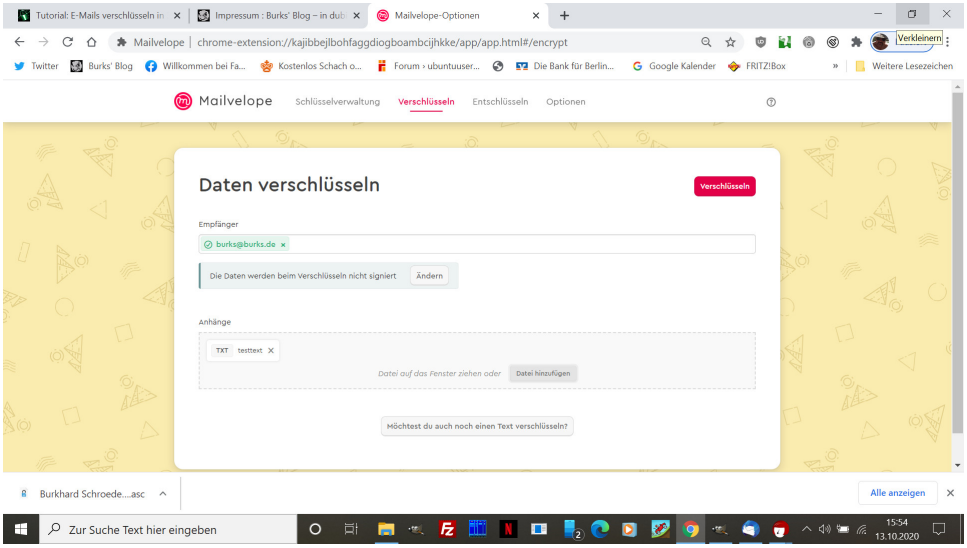


Die Grafik anklicken, um sie zu vergrößern.

Bei diesem Beispiel haben wir den öffentlichen Schlüssel von burks@burks.de genommen, Sie können aber auch den von unserem Impressum nehmen (rechte Maustaste, speichern unter).

Senden einer verschlüsselten E- Mail

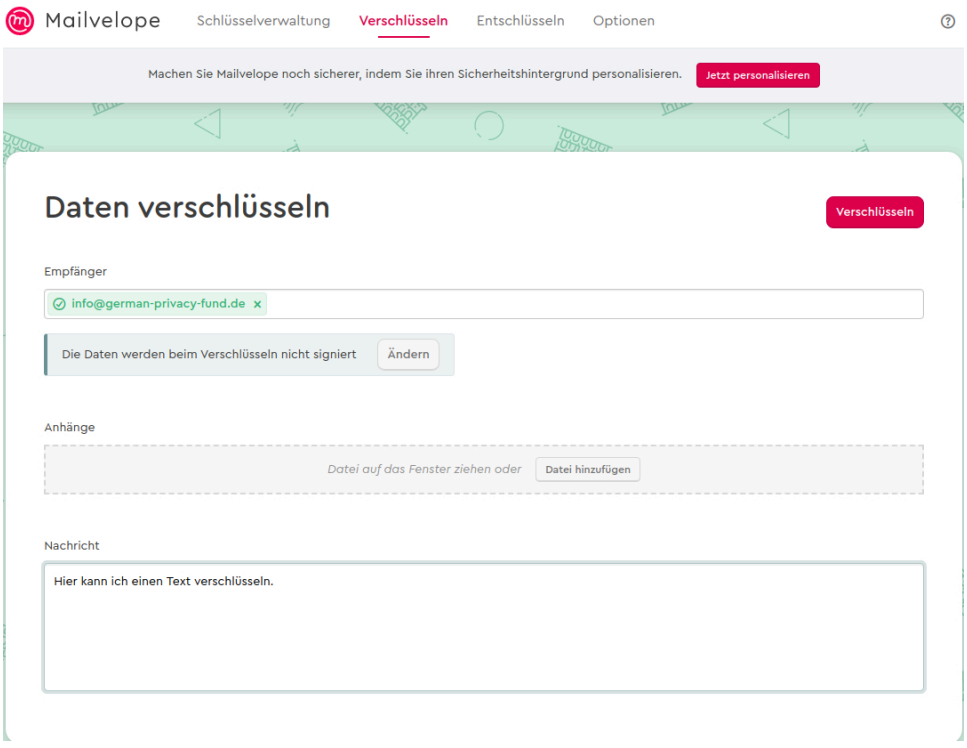
Zeitaufwand: fünf Minuten
Schwierigkeitsgrad: leicht



Die Grafik anklicken, um sie zu vergrößern.

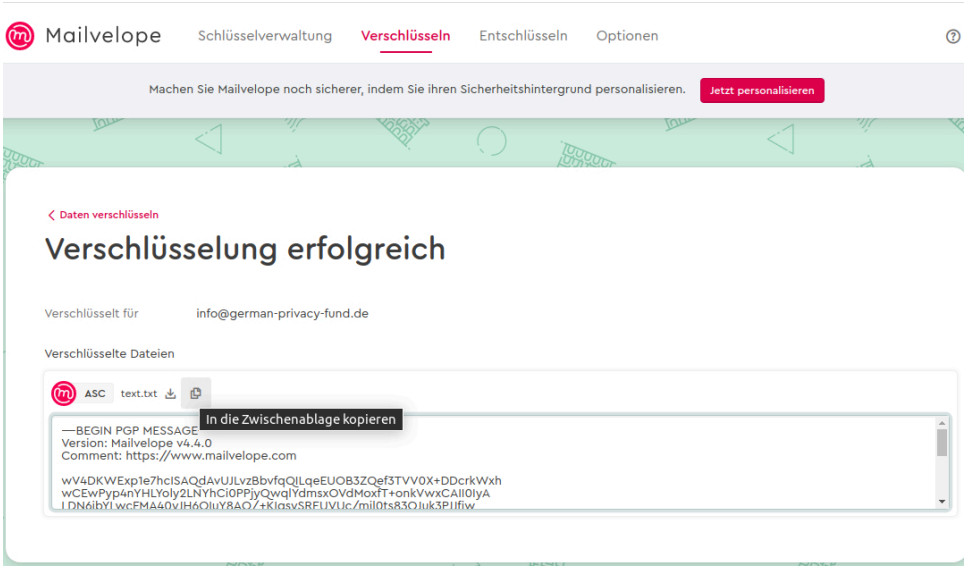
Sie können Dateien verschlüsseln (vgl. Grafik oben) und per Attachment versenden oder einen Text im Webmail-Fenster Ihres Browsers (unten).

Das Feature, den Text einer E-Mail zu verschlüsseln, verbirgt sich leider unter „Datei verschlüsseln“ und dann unter dem Button „möchtest du auch einen Text verschlüsseln?“ Dann erst öffnet sich ein Textfeld.



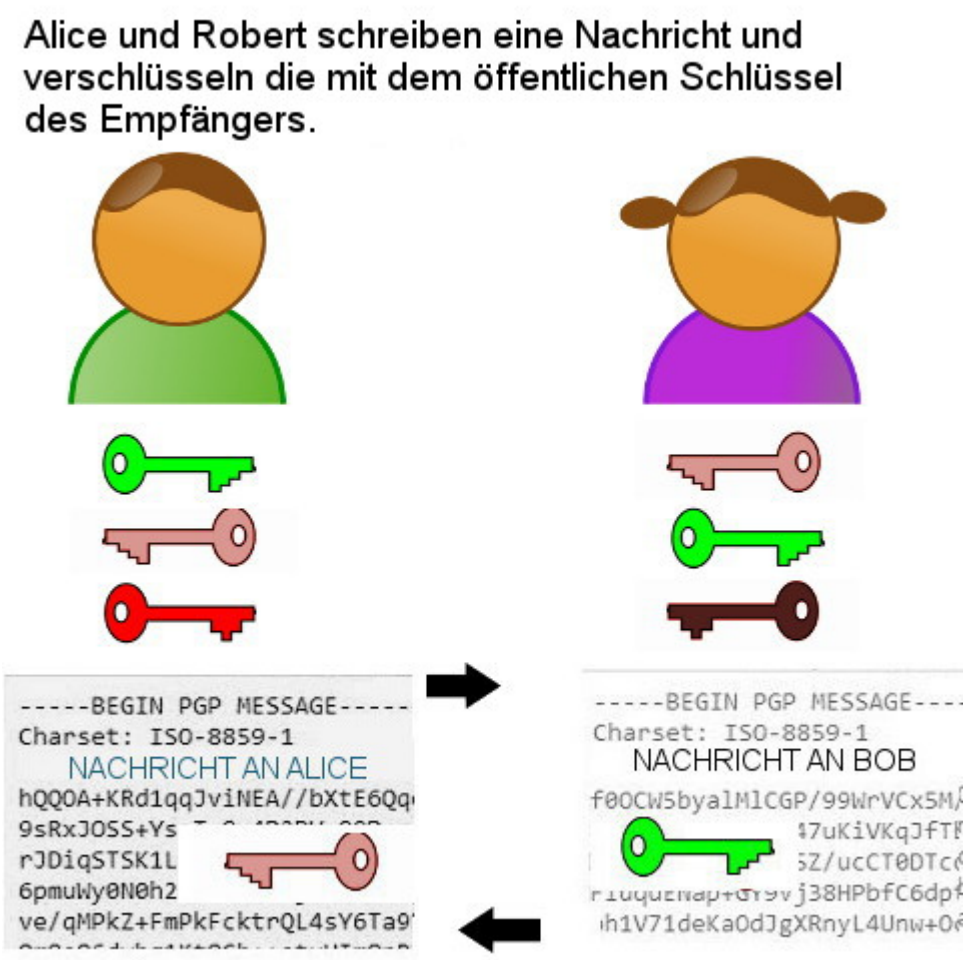
Die Grafik anklicken, um sie zu vergrößern.

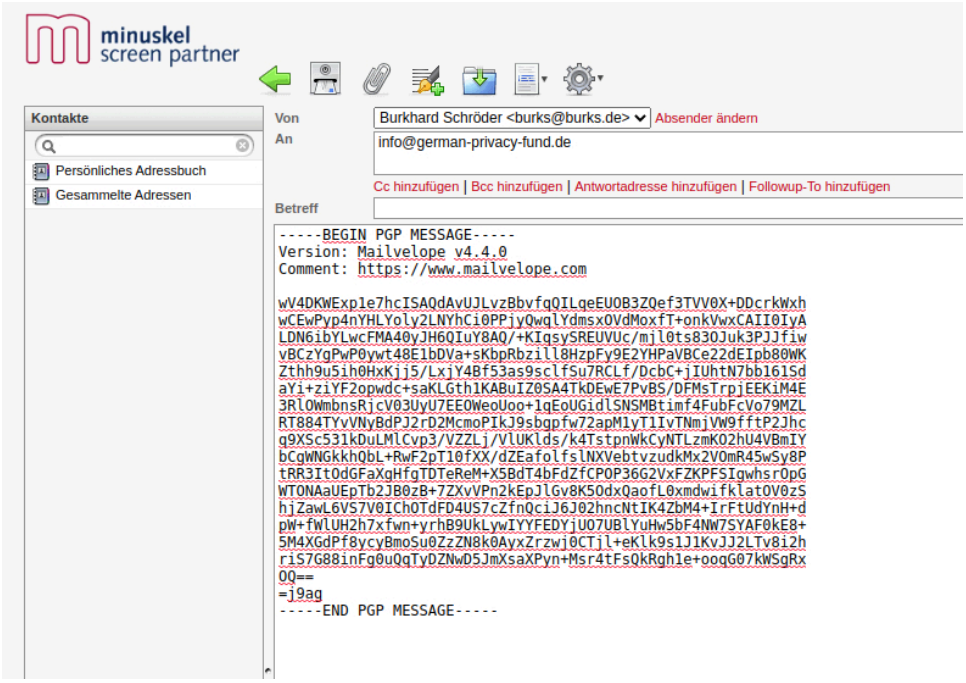
Wenn Sie den Klartext geschrieben haben, wählen Sie den Empfänger anhand seiner E-Mail-Adresse aus. Dessen Schlüssel müssen Sie schon vorher in ihr Schlüsselbund importiert haben. Dann drücken Sie auf den roten Button „verschlüsseln“ – und der Text verwandelt sich in Datensalat.



Die Grafik anklicken, um sie zu vergrößern.

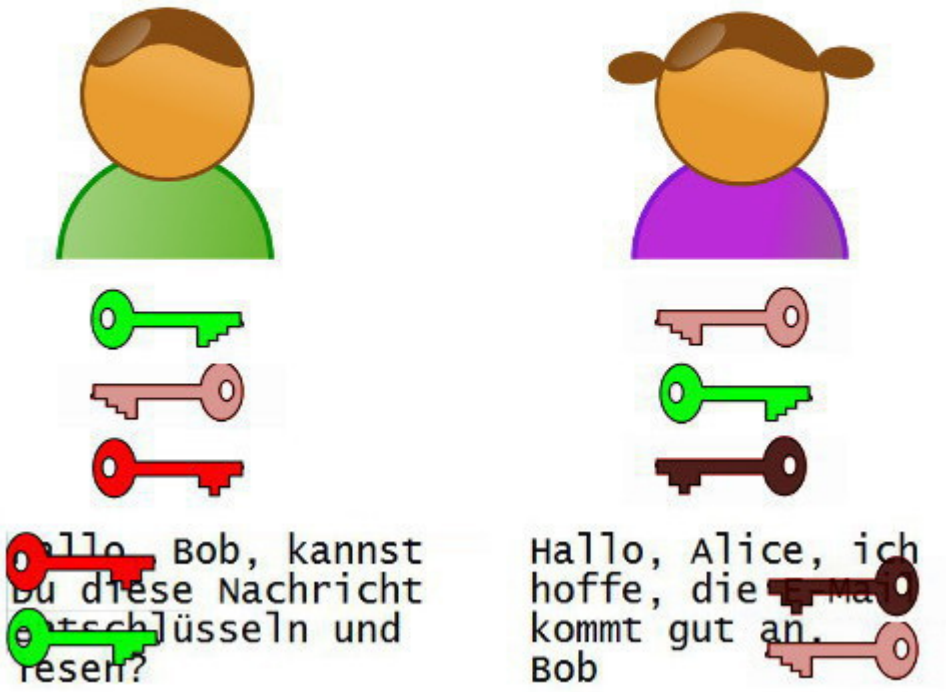
Den verschlüsselten Text kopieren Sie in das Webmail-Feld Ihres Browsers. Nur derjenige, der im Beispiel (Grafik unten) den *geheimen* Schlüssel des Empfängers info@german-privacy-fund.de hat, könnte die Nachricht wieder entschlüsseln.





Die Grafik anklicken, um sie zu vergrößern.

Robert entschlüsselt Alices Nachricht mit seinem geheimen Schlüssel - nur der passt zu dem öffentlichen Schlüssel, mit dem die Nachricht verschlüsselt worden war. Alice entschlüsselt Roberts Nachricht mit ihrem geheimen Schlüssel.



Last update: 08.12.2020