Verenkryptiert oder: Alles gut lesbar

```
Ich freue mich auf abhörsichere Kommunikation mit dir.

Viele Grüße


-----BEGIN PGP PUBLIC KEY BLOCK-----

mQENBFJ/xqQBCADSYtjlAeZU1SC/NpE7BbjqpkFCm+Sq47vFdW43DZqqwM7y07zM
qkbGqUpikHmjNR3ZMFM96PfjkgsvfpFVRT4wO5CL427iGW7/zcxisROY1TNb4zye
5OyQxxv57plTSBvQwGPcXk88Tz1IvW9iC3aa2GH0fKV7SEfuvdTHNtwhMgL74nLE
Bpxyhd4/2kTfEEC+szJEp+Hwp25TP6a5GDwKlZ4P3GyiX4hX5dH5K202ruxM8h6F
0PP+QBBIbSez5f34S3luE7myeMjRLYX1sy5zTY0TwU5kE6l+21LWG6ONt3fauVgT
Py/tkxYFAio3VWtmPfSIsS3LnzFQyybi0PgnABEBAAG0MUJlcm5kIExhbW1lbCAo
V28gd29obnRlIFZhdGVyKSA8YmVybmRAbGFtbWVsLmNvbT6JATkEEwECACMFAlJ/
xqQCGw8HCwkIBwMCAQYVCAIJCgsEFgIDAQIeAQIXgAAKCRD18rwAn1UecXfBCACH
5eDqAttWqreG8gTaCYtu3G9QoQBhjK36R0QKmWZgAgSKZPrhQDCY0TsDlE2dJhXZ
aCqPxT7YLKxm8mJF+ekkkUXfsKoGatravor9sYGAFNRnhh+xJXGVFAxfbD1yveOl
Z/ZcX5IRMqhus/EDrY3DFu969ZoMH8+jIPsasXb9g3aWLBlcKM1P4eYSNwkVXkew
2v0TCft45fn1Ccy9WZ9jDDVPyzR6uBUbE/c3FThC6Mv+d1lwewIroCAm5L5igzEz
e8+7Up31ONFe/gaftpQmQsP/zak7z83kdhtnR3OQzbX8xxyO7vJW0TZ+lugaE0pi
r6710p1EvWcYfP6Jf1/1
=3oF0
-----END PGP PUBLIC KEY BLOCK-----
```

Mit Produkten aus dem Hause Apple hatte ich noch nie zu tun, außer dass ich in meiner Zeit als Chefredakteur mit InDesign arbeiten musste. Schon seit Jahren wollte ich einen Tutorial für Mac-Produkte schreiben, wie man E-Mails verschlüsselt, bin aber mangels Hardware nie dazu gekommen. Zwei Freunde versuchten jüngst, mir verkryptografierte (ich will nur vermeiden, „verschlüsselt“ zu wiederholen) E-Mails zu schicken. Das gestaltete sich so schwierig, dass ich mich frage, ob man es überhaupt empfehlen kann.

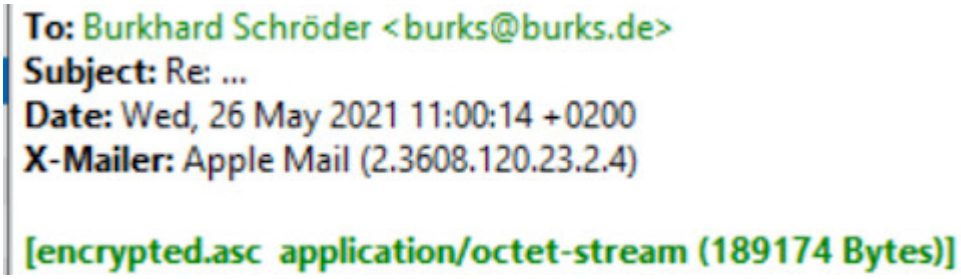
Apples „Tutorial“ ist Bullshit-Bingo vom Feinsten: Es wird weder auf den Unterschied zwischen OpenPGP und S/Mime eingegangen noch verraten, dass das Verschlüsseln offenbar nicht mehr gratis ist. Angeblich, so wurde mir berichtet, gibt es nur einen einen Zeitraum von 30 Tagen, in dem die entsprechende Software für das Standard-Programm Mail frei

verfügbar ist. Was danach? Muss man es einmalig kaufen oder gar ein Abonnement abschließen? Oder muss man auf Thunderbird ausweichen?

Andere Tutorials sind nicht pädagogisch wertvoll aufgebaut, sondern arbeiten nach dem Motto „Von-Hölzken-auf-Stöcksken“, wie man im Ruhrpott zu sagen pflegt. Macwelt: „Was zunächst kompliziert klingt, ist in der Praxis relativ einfach zu bewerkstelligen. Alles, was Sie dazu brauchen, ist ein Mailprogramm wie Apple-Mail, in dem Ihre Mailadresse bereits eingerichtet ist. Die Verschlüsselung funktioniert System übergreifend, das heißt, dass es völlig egal ist, ob Sie oder Ihr Empfänger an einem Mac oder einem PC mit Windows oder Linux sitzen.“

Glatt gelogen, Euer Ehren. Man kann Gift drauf nehmen: Wenn behauptet wird, wie in fast allen gar schröcklichen Linux-Wikis, etwas sei „einfach“, dann kapiert man das nie. Machen wir die Probe aufs Exempel: Von Mac per Mail auf Windows mit Claws Mail. Letzteres ist nur für Kaltduscher und zeigt HTML-Mails gar nicht an, sondern nur den Text. (Alle Werbeagenturen und Corporate-Identity-Fuzzies kriegen jetzt natürlich einen Anfall.)

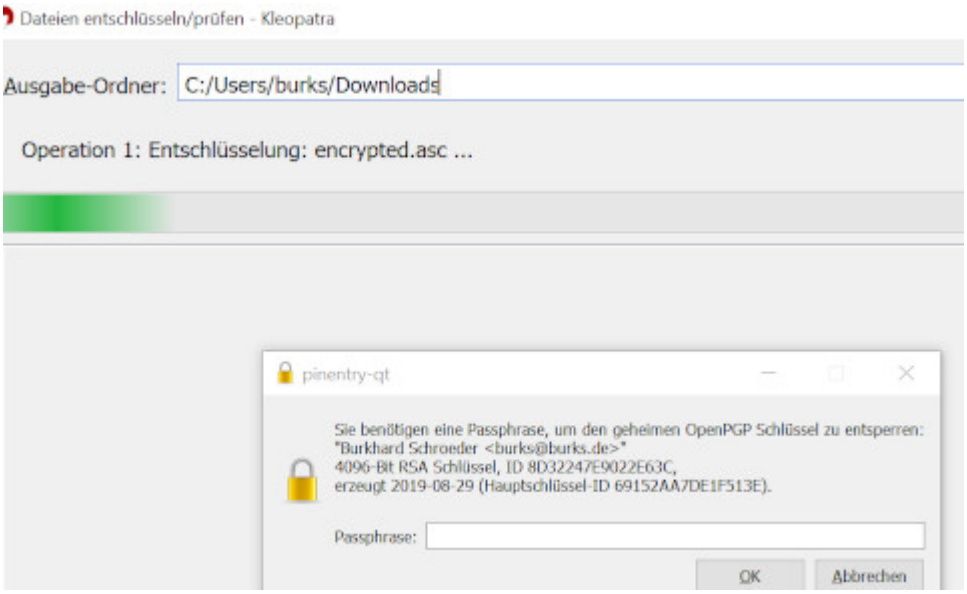
Ein Freund schickte mir also frohgemut seinen frisch erzeugten öffentlichen Schlüssel, aber leider nicht als Attachment, sondern inline – vielleicht aus Versehen. Ich wollte nicht meckern und machte mich ans Werk, eingedenk der Tatsache, dass, wenn etwas schief gegen kann, das auch garantiert passiert.



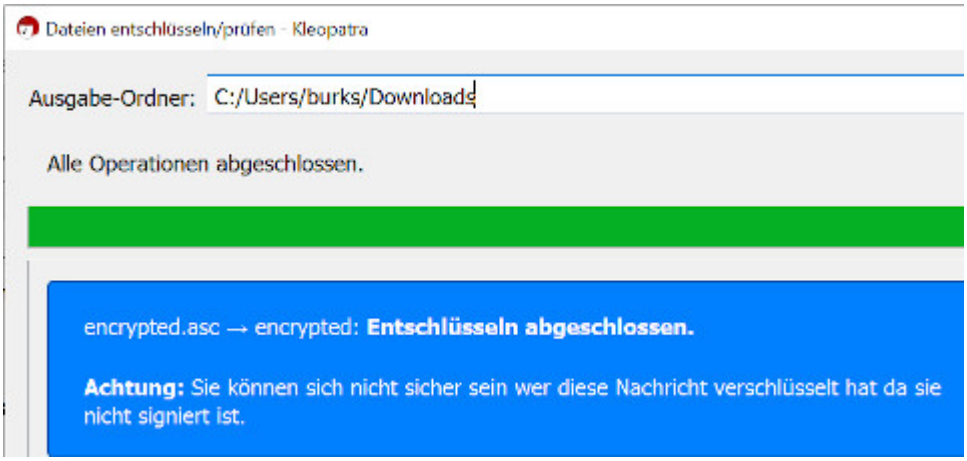
Ich kopierte also mit einem Texteditor den Schlüssel in eine

Datei, der ich die Endung asc. zuwies. (Das lernt bekanntlich jedes Kind in der Schule.) Den konnte ich dann mit Kleopatra in mein Schlüsselbund importieren. Da der normale DAU *Claws Mail* ohnehin nicht nutzen wird, weil das nicht klickibunti ist, beschwere ich mich nicht.

Ich schickte ein mit Kleopatra verschlüsseltes Attachment im Textformat zurück, weil *Claws Mail* nicht in der Lage ist, schon vorhandene Schlüssel – meine zum Beispiel – zu importieren. Auf das Verenkryptieren des E-Mails-„Körpers“ muss ich also verzichten. Danach kam gleich die erste Mail, die *Claws Mail* sehr *nerdy* als encrypted.asc anzeigt. Rechte Maustaste, speichern.



Entschlüsseln der Datei mit Kleopatra. Nach Eingabe der Passphrase meldet die Software freundlich, dass alles getan sei. Aber was jetzt? Ein Klartext war nicht zu sehen, nur im dementsprechenden Ordner eine Datei *encryptet*, von der ich ~~ums Verrecken nicht~~ nicht herausbekam, in welchem Format die war. Windows zeigt nichts an. Vielleicht kenne ich mich mit Windows auch nicht genug aus….



Also wieder der Texteditor – mit dem kann man nichts falsch machen. Lesbar. Man kann offenbar nicht alles haben. Aber warum sieht das so komisch aus? Muss das so sein? Mir Linux ging übrigens alles problemlos.