Cryptoparty Treptow

Schlüsselitits für Anfänger

Kiezini KUNGER

Mit freundlicher Unterstützung / auf Einladung von:

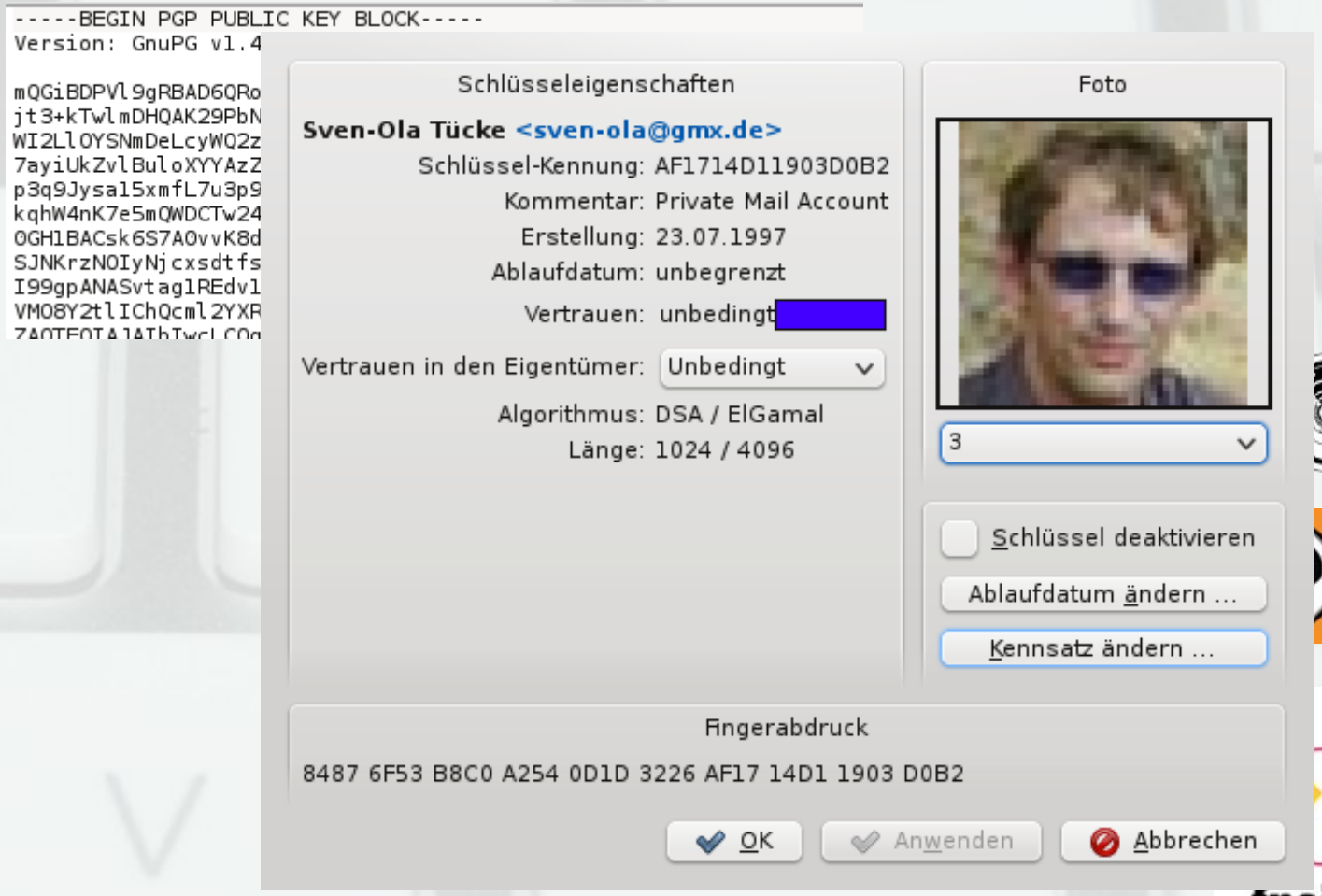
BÜNDNIS 90 DIE GRÜNEN

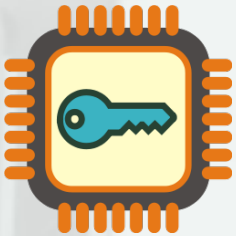
DIE LINKE.

Die PARTEI

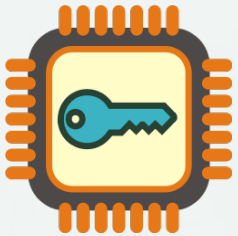
PIRATEN PARTEI

Darf ich mich vorstellen?





Crypto – was ist das?



- Verschlüsseln, entschlüsseln, beglaubigen
  (nicht manuell mit Tabellen wie früher, sondern mit Hilfe von Computern)
- Eine Technik, Sie längst täglich nutzen
  (WLAN, Software-Updates, EC-Karte, GSM-Telefonie / SIM-Karte, WLAN mit Verschlüsselung, Google-Abfrage via HTTPS, schnell löschbare Festplatten)
- Oft: Transport sichern, Anbietersicherung
  (z. B. GSM/SIM: Sie weisen nach, wer sie sind. Es gibt aber keine sichere Anbieterprüfung. Folge: Polizei und böse Buben nutzen IMSI-Catcher)
- Verschlüsselung von Person zu Person
  (das soll heute Abend hier Thema sein – Thema ist aber viel umfangreicher)

Hicks...!

Ein Beispiel

- Sie erhalten Post: einen Brief mit einer An-zeige und einem Blutalkohol-Testergebnis.
- Dies soll an Ihren Anwalt per E-Mail.
- Sie legen den Brief auf einen Scanner.
- Doch halt: E-Mail können doch viele Leute mitlesen (z. B. Arbeitgeber). Und jetzt?

Sie packen die Bilddatei in ein ZIP-Archiv mit Passwort. Sie senden die E-Mail und verraten das Passwort per Telefon. Schlau, nicht wahr? Oder doch nicht?

ZIP + Passwort: viele Haken

- Jedesmal neues Passwort. Aufschreiben?
- ZIP-Passwort „ausrechnen“: dauert wenige Stunden, für „Dienste“ gar kein Hindernis
- Mehrere Empfänger: 1 Passwort für alle
- Wenn Telefonat abgehört wird: unsicher
- Hoffentlich ist ihre Stimme bekannt.

Lösung: Da gibt’s doch was von Zimmermann. Ist aus 1991 und immer noch gut. „PGP“ für „ziemlich gute Privatsphäre“ - heute „GPG“ für „GNU Privacy Guard“

Man nehme: zwei Schlüssel

- Einer ist geheim
- Bleibt auf der Platte
- Nur für eine Person
- Zum Entschlüsseln
- Zum Signieren

- Einer ist öffentlich
- Kann in die Zeitung
- Kann jeder nutzen
- Zum Verschlüsseln
- Zur Echtheitsprüfung

Äh - ja. Das ist Mathe. Primzahlenzerlegung oder Punkte auf einer Ellipse. Große Zahlen. Hin-Rechnung geht schnell. Her-Rechnung dauert ein paar Millionen Jahre.

Schlüsselpaar (A+B) benutzen

- 1. Klartext + Schlüssel A => Geheimtext
- 2. Geheimtext + Schlüssel B => Klartext
- Geht auch anders herum (K+B=G, G+A=K)
- Einen der beiden Schlüssel veröffentlichen
- Den anderen für sich geheim behalten
- Wichtig: Schlüsselpaar **selber** erzeugen!

Die Sache mit dem Vertrauen

Vertrauen Sie mir? Der Regierung? Einer großen Software-Firma? Sich selbst? Nicht sicher? Richtig geraten: An dieser Stelle kann Geld verdient werden.

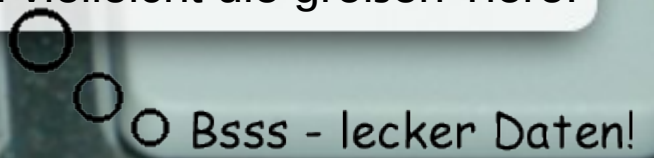
- Wer sagt Ihnen eigentlich, ob die Webseite Ihrer Bank auch wirklich von der Bank ist?
- Ach so. Ihr Browser zeigt das an. Dann schauen wir mal im Webbrowser nach.
- Und? Sagt das auch etwas darüber aus, ob Ihre Bank sicher mit dem Internet umgeht?

Mit der letzten Frage wird noch mehr Geld verdient. Ja – so ein Browser nutzt das gleiche Verfahren. Das mit den öffentlichen und den privaten Schlüsseln.

Die Sache mit der Sicherheit

- Sichere Kommunikation kann man nicht delegieren. Sie sollten es selbst machen.
- Vorsicht dubiose Verfahren; z. B. DE-Mail hat keine Ende-zu-Ende Verschlüsselung.
- Prinzipiell: Vorsicht bei Closed-Source (Apple, Google, Microsoft). Nur die Firmen wissen, welche Hintertüren drin sind.

Ja – ist bekannt: Selber machen ist unbequem. Andererseits: Wenn man einen Honigtopf aufstellt, kommen zuerst die Fliegen und dann vielleicht die großen Tiere.



Allerdings: nicht übertreiben!

- Einem Freund schreiben: einfach nutzen
- Bei einem Anwalt eine Schlüsselprüfung
- E. Snowden in der Verwandtschaft? Da sollten Sie schon Ihren Rechner säubern
- Kriegspartei? Verbrecher? Geheimdienst? Einen ordentlichen Schuss Paranoia bitte.

Es mag ja sein, dass **Sie** nichts zu verbergen haben. Dann helfen Sie anderen. Wenn eine verschlüsselte E-Mail an die Presse gleich einen Alarm auslöst, dann haben wir alle ein Problem. Und sei es nur das Problem langweiliger Berichte.

Live-Vorführung

- Zusehen bildet: E-Mail verschlüsseln und entschlüsseln am Beispiel. Soweit möglich mit PC- und Android-Software gezeigt.
- Wenn die Zeit reicht: So telefonieren Sie sicher und verschlüsselt mit SIP und ZRTP.
- Danach ist Party: Personen, die einen Rechner mitgebracht haben, können wir anschließend bei der Einrichtung helfen.

Software-Empfehlungen

Empfehlungen – natürlich geprägt von persönlichen Erfahrungen und Präferenzen

- Mail: Thunderbird von Mozilla
  (Linux, Windows, Mac OS X; im Programm das Addon „Enigmail“ installieren)
- Androiden: K9+APG, R2Mail2, Csipsimple
  (K9 kein PGP/Mime, S/Mime; R2Mail2 kostet 5 Euro; Csipsimple kann ZRTP)
- GPG4Win: Schlüsselverwaltung, Outlook
  (Bei Linux ist GPG sowieso dabei, bei Windows muss es installiert werden.)
- Telefon: Jitsi – die Alternative für Skype
  (Ist Java – aber keine Angst. Das Programm kann mit ZRTP verschlüsseln.)
- Generell: Installieren Sie Linux (Ubuntu).
  (Hat weniger Hintertüren nach allgemeiner Einschätzung, LiveCD oder USB.)

Weiterlesen im WWW

http://www.foebud.org/selbstverteidigung/
Der Verein „Digitale Courage“ (früher „Foebud“) zum Thema

http://altlasten.lutz.donnerhacke.de/mitarb/lutz/anon/pgp.html
PGP Einführung in verständlichen Worten (alt aber gut)

http://www.kes.info/archiv/online/01-01-60-SMIMEvsOpenPGP.htm
Vergleich zwischen PGP/GPG und S/MIME (E-Mail-Verschlüsselung)

https://wiki.piratenpartei.de/HowTo_Cryptoparty#Material_und_Quellen
Piratenpartei: eine Liste mit Links auf weiteren Lesestoff

http://de.wikipedia.org/wiki/Kategorie:Kryptologie
Die Wikipedia bietet (wie immer) ausreichend Lesestoff

http://www.schneier.com/
Blog eines der Crypto-Päpste (englisch und schon sehr ausführlich)

http://www.heise.de/download/sicherheit/
Software-Verzeichnis des Heise-Verlags (Zeitschriften C't, IX)