T3RMINAL.21

EIGENBAUKOMBINAT
Makerspace, Hackerspace und Mitmachwerkstatt

Grundlagen verschlüsselter Kommunikation

Lisa Krug, Frank Lanitz,
Christian Schmidt

Warum verschlüsseln?

TERMINAL.21
EIGENBAUKOMBINAT
Makerspace, Hackerspace und Mitmachwerkstatt

- Privatsphäre gilt auch im Internet
- E-Mail vergleichbar mit Postkarte
- Daten, die anfallen werden gesammelt
  - Überwachung
  - Werbung / kommerzielle Verwertung
  - Big Data
- Meinungsfreiheit
- Schutz vor Datenmissbrauch
- Schutz bei Datenverlust
- u.v.m.

GnuPG

T3RMINAL.21
EIGENBAUKOMBINAT
Makerspace, Hackerspace und Mitmachwerkstatt

- GNU Privacy Guard
- Freie Software auf Basis von OpenPGP
- PGP ursprünglich von Phil Zimmermann in den USA entwickelt
- Patente und Exportverbot für Verschlüsselung verhinderten eine Verbreitung von PGP
- Quellcode wurde als Buch veröffentlich und weltweit verkauft
- Abschriften und Scans bildeten die Grundlage für die freie Software
- Seit 1997 als OpenPGP von der IETF standardisiert

Verfahren

T3RMINAL.21
EIGENBAUKOMBINAT
Makerspace, Hackerspace und Mitmachwerkstatt

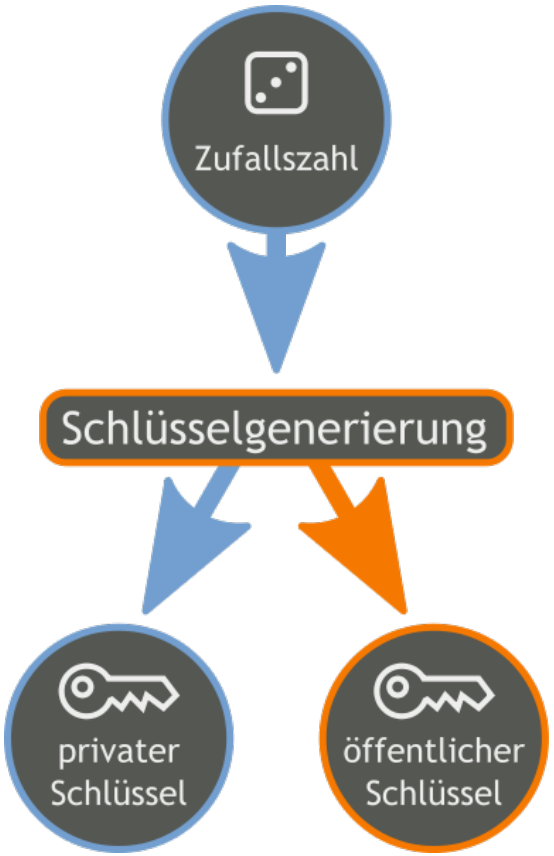
- Symmetrische Verschlüsselung
  - Verschlüsselung mit Hilfe eines Schlüssels / Geheimnises
  - Problem des Austausches und der Verwaltung
- Public-Key-Verfahren (Diffie-Hellman-Schlüsselaustausch)
  - öffentlicher (bekannter) und geheimer (privater) Teil
  - vorher kein Austausch geheimer Informationen nötig

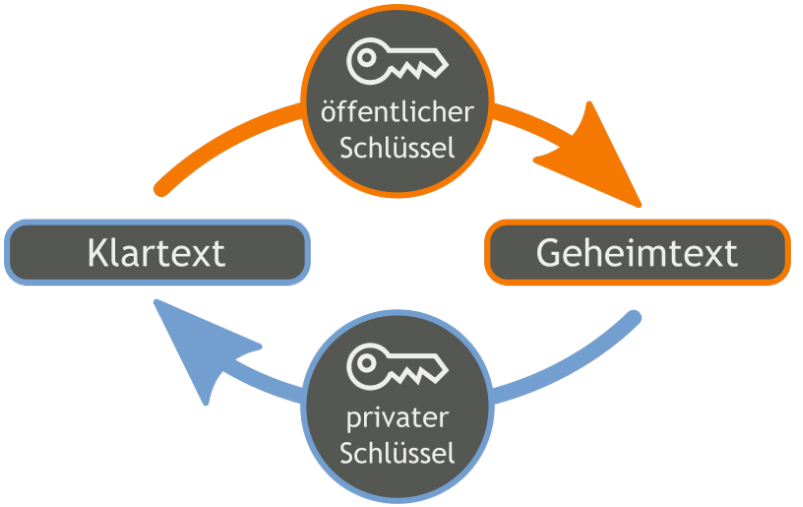
- Stiftfilm von mailbox.org
  - https://mailbox.org/stiftfilm-wie-funktioniert-e-mail-verschluesselung-mit-pgp/

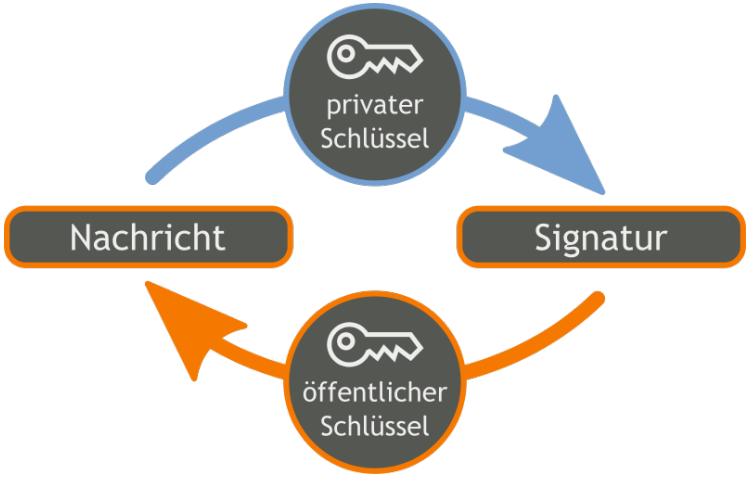
Public-Key - verschlüsseln und unterschreiben

TERMINAL.21

EIGENBAUKOMBINAT
Makerspace, Hackerspace und Mitmachwerkstatt





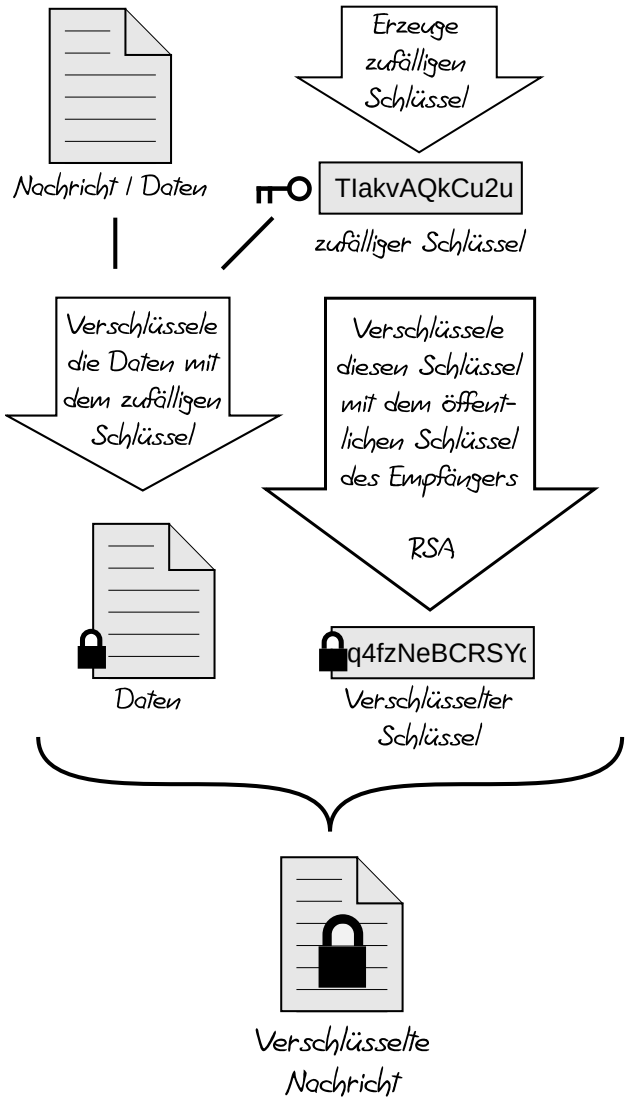


Ver- und Entschlüsseln

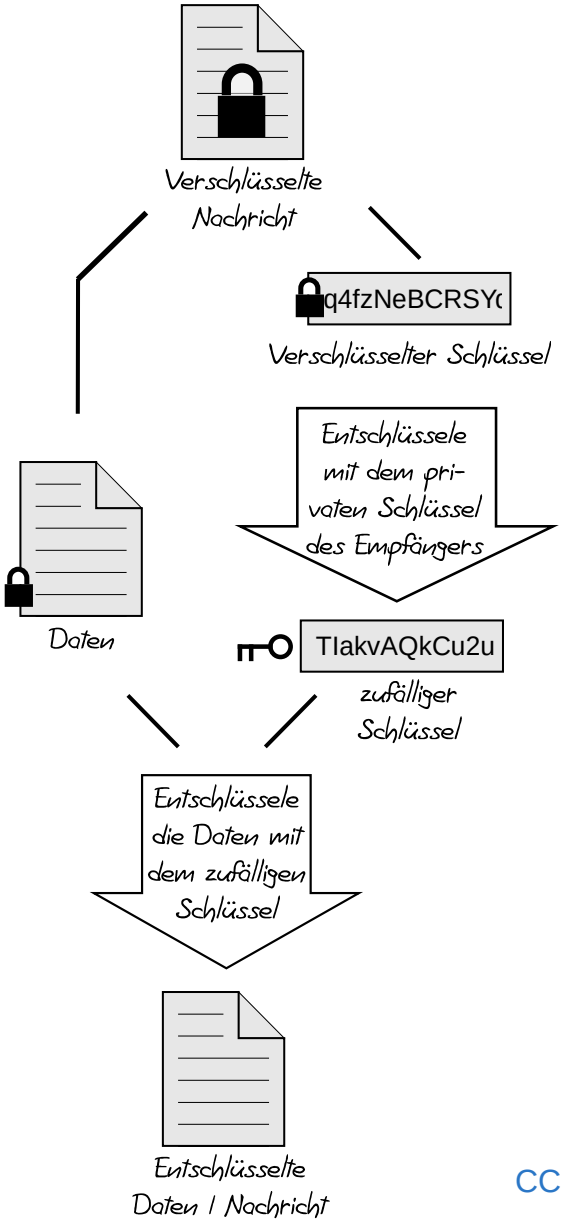
TERMINAL.21

EIGENBAUKOMBINAT
Makerspace, Hackerspace und Mitmachwerkstatt

Verschlüsselung



Entschlüsselung



Tools

T3RMINAL.21
EIGENBAUKOMBINAT
Makerspace, Hackerspace und Mitmachwerkstatt

- unterstütztes Mailprogramm
  - Thunderbird
    - https://www.mozilla.org/de/thunderbird/
  - Microsoft Outlook 2003, 2007, 2010 und 2013 (alle nur 32bit!)
- GPG Plugin
  - GPG4WIN
    - http://www.gpg4win.de/download-de.html
  - Enigmail (für Thunderbird)
    - https://addons.mozilla.org/de/thunderbird/addon/enigmail/
  - GPGTools (Mac OS X)
    - http://www.gpgtools.org/

Was kann ich tun?

TERMINAL.21
EIGENBAUKOMBINAT
Makerspace, Hackerspace und Mitmachwerkstatt

- Sicherheit ist ein Prozess und kein Zustand !
- open source Software benutzen
- Updates! Updates! Updates!
- Antivirus und „Internet Security“ Software ist Schlangenöl
  - Alternative: desinfec't
- Systeme nicht mit Administratorrechten benutzen
- Passwörter → https://xkcd.com/936/
  - offline Passwortmanager benutzen, zB KeepassXC
- HTTPS, GPG, OTR, TOR, VPN, VDS
- Dienstleistungen kosten Geld!

  → für Mail zB Posteo oder Mailbox.org (1€/Monat)

Was kann ich tun? (2)

TERMINAL.21
EIGENBAUKOMBINAT
Makerspace, Hackerspace und Mitmachwerkstatt

- datensammelnde Dienste meiden, stattdessen wenn möglich selbst betreiben
- Alternativen für gängige Dienste:
  - → Suchmaschine: DuckDuckgo, Startpage
  - → Messenger: Jabber/XMPP, Riot.im
  - → Cloud: Nextcloud, Seafile
- Informieren!
  - mich selbst und auch andere
  - das Internet geht nicht mehr weg!
  - der Weg, den wir jetzt einschlagen, beeinflusst die Zukunft unserer Gesellschaft massgeblich

Was kann ich tun? (3)

T3RMINAL.21

EIGENBAUKOMBINAT
Makerspace, Hackerspace und Mitmachwerkstatt

- Eigenbaukombinat Halle e.V. & Terminal.21 e.V.
  - Landsberger Str. 3
  - Folien unter http://download.terminal21.de/workshops/
- Linux Presentations Day 2 mal pro Jahr
  - Linux ausprobieren und kennelernen
- Ausbildung muss sich ändern! Bitkom vom 03.11.2015:
  - Bitkom-Hauptgeschäftsführer Dr. Bernhard Rohleder warnt jedoch, dass "alle Berufe, vom Handel über die Industrie bis hin zum Handwerk" von der digitalen Transformation betroffen seien. Entsprechend fordert er die schulische Bildung, "mit einer fundierten Vermittlung von Digitalkompetenz im Fächerkanon, einem Pflichtfach Informatik und mit Englisch als Lingua franca der digitalen Welt ab der 1. Klasse".

    http://www.heise.de/newsticker/meldung/Bitkom-Digitalisierung-veraendert-die-Berufsausbildung-2868964.html

- Humans need not apply! https://www.youtube.com/watch?v=7Pq-S557XQU

Links

TERMINAL.21
EIGENBAUKOMBINAT
Makerspace, Hackerspace und Mitmachwerkstatt

- ausführliche Folien von einem älteren Vortrag http://download.terminal21.de/workshops/swap2015/Sicherheit_im_Internet.pdf
- Ratgeber: was gegen die NSA gut ist, ist auch gegen Überwachung gut https://prism-break.org/en/
- umfangreiche Hintergrundinformationen und Instruktionen auf Deutsch gegen Überwachung https://www.privacy-handbuch.de/print.htm
- Browser-Addons:
  - https://noscript.net/getit (Java Script & mehr verbieten)
  - https://addons.mozilla.org/de/firefox/addon/ublock-origin/ (gegen Trackingdienste, ist gegenüber ghostery zu bevorzugen)
  - https://www.eff.org/https-everywhere (HTTPS Verbindungen erzwingen, wenn verfügbar)
- wer dich beim Nachrichtenlesen trackt https://trackography.org/
- Ratgeber: unterwegs im öffentlichlichen WLAN
  - Web: https://www.mbem.nrw/unterwegs-im-oeffentlichen-wlan-aber-gut-geschuetzt
  - PDF: https://mbem.nrw/sites/default/files/asset/document/ratgeber_-_unterwegs_im_oeffentlichen_wlan_0.pdf

Keys und Fingerprints

T3RMINAL.21
EIGENBAUKOMBINAT
Makerspace, Hackerspace und Mitmachwerkstatt

- Lisa Krug:

  Lisa.Krug@gmx.net

  513F 1E62 36CC 8006 DC16 F964 53C9 7193 30D8 F483

- Frank Lanitz

  frank@lanitz.info

  CD38 C008 828C 2EF1 B63A 8ED1 B568 8B00 6F78 F01E

- Christian Schmidt

  christian@terminal21.de

  C6FA A119 1378 B42D 0025 813F 3397 B76E D838 C16C