

Ziemlich gute Privatsphäre



Eine Einführung in die sichere Kommunikation
mit PGP/GnuPG und Delta Chat

Ulf Treger @ Didays, 2.10.2028 in Hamburg- Harburg

Themen

1. Ziemlich gute Privatsphäre
 1. ... ein paar Begriffe
 2. Wozu brauche ich PGP/GnuPG?
 3. Geschichte (PGP 1991)
 4. Geschichte (OpenPGP 1998)
 5. Geschichte (GnuPG)
 6. Geschichte (PGP/GPG heute)
 7. Asymmetrische Verschlüsselung
 8. Checkliste
 9. Delta Chat ...nicht noch ein Messenger! Doch :)
10. Danke

... ein paar Begriffe

→ Kryptografie

„Verborgen schreiben“ — die Wissenschaft der Verschlüsselung von Informationen

→ Verschlüsselung

Die Umwandlung von „Klartext“ (für alle lesbar) in einen geheimen Text (nur lesbar für Menschen, die einen Schlüssel haben um den Text zu entschlüsseln). Gegenteil von Entschlüsselung ;)

→ Schlüssel

Das Verfahren, mit dem ich einen Text ver- oder entschlüsseln kann.

Klassische Verschlüsselung (vor-digital) bedingte, dass Sendende und Empfangende sich auf einen Schlüssel einigen (Etwa: Ein Buch + ein Verfahren dieses zu nutzen: der geheime Text enthält Angaben zu Seitenzahl und Position eines Buchstabens, woraus ich eine Botschaft bauen kann)

Wozu das ganze?

E-Mail Verschlüsselung als ein Element der digitalen Selbstbestimmung:

→ Privatsphäre

Ich möchte selbst entscheiden, welche meiner Äußerungen oder Daten öffentlich sind und welche privat bleiben.

→ Vertraulichkeit

Ich möchte Informationen an jemanden schicken und möglichst sicher sein, dass nur die adressierte Person sie lesen kann.

→ Authentizität

Ich möchte überprüfen können, ob eine Information wirklich von einer bestimmten Person kommt.

Verschlüsselungssoftware

👤 Entwickler:
Phil Zimmermann

PGP 1991
„Pretty Good Privacy“

🔑 128 Bit Schlüssellänge



§ Freeware, dann
Proprietär

Standard für verschlüsselte und
digital signierte Daten

OpenPGP¹⁹⁹⁸

Verschlüsselungssoftware

👤 Entwickler:
Phil Zimmermann

PGP¹⁹⁹¹
„Pretty Good Privacy“

🔑 128 Bit Schlüssellänge



§ Freeware, dann
Proprietär

Verschlüsselungssoftware

👥 Entwickler*innen:
The GNU Privacy Guard Team

seit 1997

GnuPG
„GNU Privacy Guard“

🔑 3072 bis 4096-Bit Schlüssellänge (RSA)



§ Free Software
GNU GPL

Standard für verschlüsselte und
digital signierte Daten

OpenPGP 1998

Verschlüsselungssoftware

👤 Entwickler:
Phil Zimmermann

PGP 1991
„Pretty Good Privacy“

🔑 128 Bit Schlüssellänge



§ Freeware, dann
Proprietär

Verschlüsselungssoftware

🐾 Entwickler*innen:
The GNU Privacy Guard Team

GnuPG^{seit 1997}
„GNU Privacy Guard“

Thunderbird
für Desktop
\$ Free Software

mit Engimail (bis 2018)

K-9 Mail
für Android/F-Droid
\$ Free Software
Apache Licence

mit OpenKeychain App

Webmailer:
Posteo, Proton

Standard für verschlüsselte und
digital signierte Daten

OpenPGP¹⁹⁹⁸

Verschlüsselungssoftware

👤 Entwickler:
Phil Zimmermann

PGP¹⁹⁹¹
„Pretty Good Privacy“

🔑 128 Bit Schlüssellänge



\$ Freeware, dann
Proprietär

Asymmetrische Verschlüsselung

Public-Key-Kryptographie


öffentlicher
Schlüssel
„Public Key“




privater
Schlüssel
„Secret Key“



Asymmetrische Verschlüsselung

Public-Key-Kryptographie



öffentlicher Schlüssel
„Public Key“
Jede*r kann damit eine Nachricht
(für mich) verschlüsseln



Nur ich kann diese Nachricht
mit meinem privaten Schlüssel
entschlüsseln.

privater Schlüssel
„Secret Key“

Checkliste für die Benutzung

Asymmetrische Verschlüsselung mit GnuPG

- Eigenes Schlüsselpaar erzeugen
- (Einen „Revocation Key“ erzeugen)
- Den eigenen öffentlichen Schlüssel verteilen
- Die öffentlichen Schlüssel von anderen einsammeln
- Einem anderen Schlüssel das „Vertrauen“ aussprechen
- Nach einem anderen öffentlichen Schlüssel (im Netz) suchen
- Eine Nachricht verschlüsseln, senden und eine Antwort empfangen



OpenKeychain (Android)



Thunderbird Mobile (Android)

Andere Programme für Linux, Windows, Mac, Android, iOS: <https://www.openpgp.org/software/>

Delta Chat ...nicht noch ein Messenger! Doch :)

Delta Chat kommt mit ein paar spannenden Eigenschaften:

- basiert auf offenen Standards und bestehender Infrastruktur für E-Mails (SMTP und IMAP)
- nutzt mit OpenPGP (und Autocrypt) starke Kryptografie
- ist dezentral
- kann auf mehreren Geräten installiert werden
- kann anonym und ohne Anmeldung oder Angabe einer Telefonnummer genutzt werden
- ermöglicht das Erstellen und Einbetten von Apps, kleinen Webanwendungen die in Chats inkludiert werden können.



delta.chat

Danke!

Ulf Treger <ulf.treger@dekoder.de>

city/data/explosion

Veranstaltungen und Projekte zu Stadt, Digitalisierung

Mastodon: @citydata@mastodon.online

... und schaut bei <https://di.day/> vorbei, mit hilfreichen Wechsel-Rezepten und Veranstaltungen jeden 1. Sonntag im Monat zur digitalen Unabhängigkeit :)