

Workshop PGP

1. Anleitung

1. Überlege dir ein gutes Passwort

- min. 8 Zeichen, große und kleine Buchstaben, Zahlen und Sonderzeichen
 - Tipp: Verwende sinnlose alberne Passphrasen gespickt mit Abkürzungen und Sonderzeichen. Klar, klingt albern, bleibt aber im Kopf 😊
 - falls es dir leichter fällt: Eine lange Passphrase (20 Zeichen und mehr) ohne Zahlen und Sonderzeichen ist immer noch ziemlich gut (auf jeden Fall besser als nur 8 Zeichen)
- Noch besser ist es ausschließlich Passwörter mit min. 20 Zufallszeichen (Buchstaben, Zahlen, Sonderzeichen) zu nutzen. In Kombination mit einem Passwort Manager (z.B. [Keepass](#)) ist das eine der sichersten und komfortabelsten Varianten sich um seinen Passwortschutz zu kümmern.

2. Installiere Thunderbird

- Windows:
 - Installer herunterladen: <https://www.thunderbird.net/de/>
 - exe-Datei ausführen und Thunderbird installieren
- GNU/Linux:
 - ```
sudo apt-get install thunderbird thunderbird-locale-de
```

### 3. Installiere gpg4win

- Windows:
    - Installer herunterladen:  
<https://www.gpg4win.org/download.html>
    - exe-Datei ausführen und gpg4win installieren
  - GNU/Linux:
    - `sudo apt-get install gnupg`
4. Füge zu Thunderbird das Add-on *Enigmail* hinzu
- <https://www.enigmail.net/index.php/en/> oder
  - <https://addons.mozilla.org/de/thunderbird/addon/enigmail/>
5. Nach dem erfolgreichen installieren von *Enigmail* öffnet sich ein Assistent zum Einrichten eines PGP-Schlüsselpaares. Folge dem Assistenten und verwende einfach die Standardeinstellungen. Am Ende dieses Schritts ist die Einrichtung abgeschlossen und E-Mails können verschlüsselt und entschlüsselt werden.
6. Um die Verwendung der PGP-Verschlüsselung noch etwas komfortabler zu gestalten, können noch die folgenden Einstellungen in Thunderbird getroffen werden.
- Menü > Einstellungen > Kontoeinstellungen > OpenPGP-Sicherheit:
    - ✓ Nachrichten standardmäßig verschlüsseln
  - Neue E-Mail > Menü > Ansicht > Symbolleiste > Anpassen:
    - Füge die Buttons *Verschlüsseln*, *Nachricht signieren* und *Eigenen Schlüssel anhängen* per Drag-and-drop zur Symbolleiste hinzu.
    - Die hinzugefügten Symbole zeigen an, ob die Nachricht verschlüsselt und/oder signiert wurde sowie, ob der eigene öffentliche Schlüssel mit angehängen worden ist. Das ist übersichtlich und praktisch!

Tabelle 1 : Passwort Beispiele mit der Passphrasen Methode

| Klartext                              | Passwort                          |
|---------------------------------------|-----------------------------------|
| Da ist Zahnwachs im Föhn              | *dA1stZahn-Wach5imfö(h)n*         |
| Wer die Hunde kennt braucht kein Bier | !WerdieHundekenntbrauchtkeinBier! |
| Kugeln und Würfel schmecken Nachts    | Kugeln&Würfel->schmeckenn8s++     |

## 2. Weblinks

- Schönes einfaches Erklärvideo zu PGP
  - <https://www.youtube.com/watch?v=tamRqD43D3o>
- Gute interaktive PGP Erklärseite von Jugend hackt
  - <https://howtopgp.jugendhackt.de/#/>
- Schritt für Schritt Videoanleitung für Thunderbird in Windows
  - <https://youtu.be/ieuHHu4MoMo>
- Schritt für Schritt Anleitung für Windows, Mac, Android und iPhone
  - <https://netzpolitik.org/2013/anleitung-so-verschlusselt-ihr-eure-emails-mit-pgp/>
- Eine sehr ausführliche Erklärung in 8 Eskalationsstufen
  - <https://blogs.itemis.com/de/openpgp-im-berufsalltag-teil-1-was-ist-das>