

# E-Mail-Crypto mit GPG

## 1 Warum GPG

- Es kann deine Mails vor vor neugierigen Menschen (oder Server-Betreibern) schützen
- Es gibt dir die Möglichkeit sicher zu gehen das an der Mail unterwegs niemand “Fehler korrigiert” hat
- Du kannst sicherstellen das die Mail auch von dem kommt der vorgibt sie Geschrieben zu haben
- Du musst jemand nicht unbedingt direkt kennen um ihm zu Vertrauen (Web of Trust)

## 2 Ein Kurzer Überblick über die Funktionsweise von GPG/PGP

- GPG ist ein asymmetrisches Verfahren, das heißt ein Schlüssel besteht aus zwei Teilen: Dem *geheimen* Teil, den niemand außer dir kennen darf, und dem *öffentlichen* Teil, den möglichst viele Leute kennen sollten
- Das Bekanntgeben des öffentlichen Teils des Schlüssels ist sicher, da zur Erzeugung des Schlüsselpaares mathematische “Einwegfunktionen” verwendet werden (Es handelt sich nicht wirklich um Einwegfunktionen, aber das umkehren der Funktionen ist nicht trivial und erfordert *sehr* viel Rechenleistung und Zeit)

## 3 Wie mache ich GPG?

- Windows: Die nötigen Tools können von “GPG4Win” <http://www.gpg4win.de/> heruntergeladen werden.
- test
  - Benutzt du Thunderbird: Siehe “GPG mit Thunderbird”
  - Benutzt du Outlook: Schau im von GPG4Win installierten Kompendium nach wie man “GpgOL”, das Outlook Plugin, einrichtet
- MacOS: Die nötigen Tools können von von “GPGTools” <https://gpgtools.org> heruntergeladen werden (GPG Suite).
  - Benutzt du Mail.app/iMail: GPG Suite integriert sich automatisch in iMail
  - Benutzt du Thunderbird: Siehe “GPG mit Thunderbird”
- Linux: Die nötigen Tools sollten schon installiert sein
  - Benutzt du Thunderbird: Siehe “GPG mit Thunderbird”

## 4 GPG mit Thunderbird

- GPG wird von Thunderbird mittels der Erweiterung *Enigmail* unterstützt, diese kann unter Linux mittels der Paketverwaltung installiert werden. Unter allen anderen Betriebssystemen kann Enigmail mittels des Erweiterungsmanagers von Thunderbird installiert werden.
- In Thunderbird findest du in der Menüleiste einen Punkt “OpenPGP” in dem du die Einstellungen und Funktionen von GPG findest
- Unter dem Menüpunkt “Schlüssel verwalten...” findest du eine Liste aller Schlüssel in deinem Schlüsselbund (also deinen eigenen Schlüssel und alle die du von anderen importiert hast)
- In dem Fenster kannst du einen neues Schlüsselpaar unter “Erzeugen”→“Neues Schlüsselpaar...” erzeugen
- Unter “Schlüssel-Server”→“Schlüssel Suchen...” kannst du Schlüssel von anderen Menschen importieren
- Wenn du auf einen Schlüsseleintrag (auch euren eigenen) rechtsklickst kannst du den Schlüssel unterschreiben oder die Vertrauensstufe eines Schlüssels ändern
- Wenn du einen Schlüssel unterschreibt solltest du den unterschriebenen Schlüssel auch wieder dem Eigentümer zukommen lassen. Wenn du den Schlüssel von einem Keyserver heruntergeladen hast kannst du dem Schlüssel mit “Rechtsklick”→“Auf Schlüssel-Server Hochladen...” auf einen Server hochladen. Alternativ kannst du den Schlüssel auch mit “Rechtsklick”→“Öffentlichen Schlüssel per E-Mail senden...” per E-Mail an den Eigentümer senden.
- Wenn du eine Nachricht schreibst, kannst du entweder durch anklicken des OpenPGP Buttons oder über das Schlüssel- bzw. Stiftsymbol in der Statusleiste deine Nachricht signieren und/oder verschlüsseln.

## 5 Dinge auf die du beim Schlüssel Signieren achten solltest

- Überprüfe ob der Fingerprint des zu Signierenden Schlüssels korrekt ist, z.B. durch abwechselndes, gegenseitiges Vorlesens des Fingerprints.
- Lass dir von deinem gegenüber einen (amtlichen) Lichtbildausweis zeigen und prüfe ob die Sicherheitsmerkmale korrekt sind (wenn vorhanden).

## 6 Keyserver und Lebensdauer eines Schlüssels

Der Austausch von Schlüsseln erfolgt mittels sogenannter Keyserver. Ein Keyserver ist prinzipiell so etwas wie ein Telefonbuch, jedoch kann dort jeder selbstständig neue Einträge hinzufügen oder aktualisieren. Ein Schlüssel kann, nachdem er auf einem Keyserver veröffentlicht wurde, in der Regel nicht mehr Löschen. Daher ist es wichtig ein *Wiederrufszertifikat* zu erstellen, mit dem ein Schlüssel als ungültig markiert werden kann. Dieses Zertifikat sollte an einem sicheren Ort aufbewahrt werden.

Wichtige Keyserver sind:

- `pool.sks-keyservers.net` – Der größte Keyserver Pool, besteht aus vielen Keyservern, die sich untereinander Synchronisieren. Verwende diesen Keyserver im Normalen Betrieb und nach der Cryptoparty.
- `osak.fsmpi.rwth-aachen.de` – Keyserver der Fachschaft. Synchronisiert sich nicht mit dem Pool und ist für das Keysigning vor Ort vorgesehen.

## 7 GPG auf der Kommandozeile

- `gpg --gen-key` Neues Schlüsselpaar erzeugen.
- `gpg --gen-revoke <key_id>` Wiederrufszertifikat für euren Schlüssel erstellen. Dies ist wichtig, solltet ihr den Key nicht mehr Benutzen oder sollte der private Teil des Schlüssels kompromittiert werden
- `gpg --fingerprint <key_id>` Zeigt den Fingerprint des angegebenen Schlüssels an.
- `gpg --keyserver <server> --send-keys <key_id>` Euren Schlüssel (oder den von anderen) auf einem Keyserver veröffentlichen (z.B. `pool.sks-keyservers.net`)
- `gpg --keyserver <server> --search-keys <name>` Nach Schlüsseln von anderen auf einem Keyserver suchen
- `gpg --recv-keys <key_id>` Schlüssel herunterladen
- `gpg --sign-key <key_id>` Schlüssel unterschreiben
- `gpg --encrypt --recipient <email> <filename>` Datei verschlüsseln
- `gpg --output <decrypted_file> --dectypt <encrypted_file>` Verschlüsselte Datei entschlüsseln
- `gpg --sign --detatch-sign <filename>` Dateien unterschreiben und die Unterschrift außerhalb der Datei als `filename.sig` ablegen (wichtig bei Dateien die allergisch auf Veränderungen sind (Binärdaten))
- `gpg --verify <filename[.sig]>` Signatur einer Datei überprüfen (bei externer Signaturdatei sollte diese im selben Verzeichnis liegen)
- `gpg --edit-key <key_id>` Schlüssel interaktiv bearbeiten
- `gpg --edit-key <key_id> show` Informationen zu eurem Schlüssel anzeigen
- `gpg --edit-key <key_id> adduid` User ID hinzufügen
- `gpg --edit-key <key_id> revuid <num>` User-ID entfernen