Verschlüsselung mit GnuPG (PGP)

Vorbemerkung:
Der Datenschutz verlangt von uns einen sehr umsichtigen Umgang mit dienstlichen Daten. Dazu gehören Informationen über Schüler (wie sie in kommentierten Sitzplänen notiert werden). Insgesamt gilt das Gebot der Datensparsamkeit.

Digitale Kommunikation ist oft bequemer als andere Wege. Das gilt insbesondere für Terminabsprachen (wo ich allerdings die unmittelbare Absprache im Fachseminar oder nach einem UB vorziehe) und das Verteilen von Unterrichtsentwürfen (Einsparen von Kopien, außerdem kann ich einen vorab enthaltenen Entwurf auch vorab durcharbeiten).

Eine Email wird gerne mit einer Postkarte verglichen. Jeder kann sie lesen, wenn er Zugang zu einem der Server hat, über den die Email läuft. Für in Europa stehende Server (physischer Standort) gilt das europäische Datenschutzrecht (DGVO). Bei europäischen Email-Providern ist die Email aus Datenschutzsicht besser aufgehoben als bei außereuropäischen.

Damit wir uns sicher sein können, dass niemand unsere dienstlichen Emails lesen kann, werden wir sie verschlüsseln.
Wir nutzen dazu GnuPG.

Unten finden Sie Hinweise auf Internetseiten, die die Verschlüsselung mit GnuPG näher erklären.

Im Grundsatz funktioniert die Verschlüsselung so:
1. Sie verfassen ihre Email.
2. Sie verschlüsseln die Email auf ihrem Computer. Dazu nutzen sie einen Schlüssel des Emailempfängers.
3. Sie versenden die verschlüsselte Email.
4. Der Empfänger lädt die Email auf seinen Computer und entschlüsselt sie mit seinem Schlüssel.

Sie brauchen:
- Einen Email-Client. Das ist eine Software, mit der Sie Emails vom Provider/ Emailpostfach abrufen und auf ihren PC holen. Meine Empfehlung: Mozilla Thunderbird.
- Das Thunderbird-Plugin Enigmail.
- Einen öffentlichen und einen privaten GnuPg-Schlüssel (ein „Schlüsselpaar).
- Den öffentlichen Schlüssel des Emailempfängers.
- Aufpassen: Der Schlüssel ist spezifisch für eine bestimmte Emailadresse, bei anderen Adressen des selben Empfängers funktioniert er nicht.

Was passiert?
- Sie erzeugen ihr Schlüsselpaar
- Sie verteilen ihren öffentlichen Schlüssel an alle, die ihnen eine verschlüsselte Email schicken sollen. Im Fachseminar können Sie ihren Schlüssel z.B. in die dropbox hochladen, dort gibt es ein Verzeichnis dafür.
- Sie importieren die öffentlichen Schlüssel der relevanten Empfänger in ihre Schlüsselverwaltung (z.B. Enigmail).
- Emails an Empfänger, deren Schlüssel sie haben, werden automatisch verschlüsselt gesendet. (Beachten Sie dazu das Symbol unten links in Thunderbird).

Hier finden Sie genauere Hinweise und Anleitungen:

- zu dienstlichen Emails: https://www.datenschutzzentrum.de/artikel/901-Dienstliche-Nutzung-von-E-Mail-durch-Lehrkraefte.html
  (aus Schleswig-Holstein; Für Niedersachsen gibt es vom Landesdatenschutzbeauftragten einen Hinweis auf dienstliche Emails:
  https://www.lfd.niedersachsen.de/technik_und_organisation/orientierungshilfen_und_handlungsempfehlungen/gefahren_bei_email/e-mailaber-sicher-56145.html)

- Zur Verschlüsselung mit GnuPG
  - https://wiki.piratenpartei.de/HowTo_Emails_verschlüsseln_mit_PGP_mit_Thunderbird
    (ich verbinde damit keinesfalls eine politische Botschaft, aber diese Anleitung ist gelungen)
  - https://support.mozilla.org/de/kb/nachrichten-digital-signieren-und-verschlusseln
  - https://t3n.de/magazin/pgp-gpg-einsatz-e-mail-verschluesselung-leicht-gemacht-234668/
  - https://emailselfdefense.fsf.org/de/index.html
    (sehr übersichtlich. Hier findet sich auf ein Link zu **Edward**)

Bei Schwierigkeiten dürfen Sie mich gerne ansprechen.

Zum Testen der Verschlüsselung können sie mit dem Email-Roboter Edward kommunizieren (siehe Link auf https://emailselfdefense.fsf.org/de/index.html).

Zum weiteren Test dürfen Sie mir gerne eine oder mehrere Emails schicken.