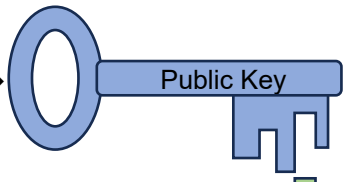
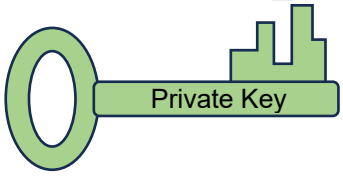
Verschlüsselung von Mails mittels PGP 2026-07

Der Inhalt einer E-Mail wird verschlüssselt und als verschlüsselte Datei mit einem beliebigen E-Mail-Programm verschickt.

- Das **Verschlüsseln** erfolgt beim Sender mit dem **Public Key des Empfängers** →



- Das **Entschlüsseln** erfolgt beim Empfänger mit **seinem Private Key** →



E-Mail-Empfänger
- Sowohl der Public Key als auch der Private Key wird zunächst beim Empfänger erzeugt.
- Den Public Key sendet er an humans.international.
- Der Private Key verbleibt **nur** beim Empfänger.

E-Mail-Sender
- Der Sender lädt bei humans.international den Public Key vom Empfänger herunter.
- Er verschlüsselt damit den Inhalt der E-Mail und erzeugt eine verschlüsselte Datei.
- Diese Datei versendet er mit einem beliebigen E-Mail-Programm.

Empfänger:
- Nur er kann den E-Mail-Inhalt mit seinem Private Key entschlüsseln, der zum Public Key passt.

Allgemein:
- Sender und Empfänger müssen verifizierte Personen sein.
- Eine Person kann sich als Privat-Person verifizieren lassen (MaxMustermann**1**DE mit Verifizierungs-Adresse zuhause) und zusätzlich in einer Firma als handelnde Person (MaxMustermann**2**DE mit Verifizierungs-Adresse in der Firma).
  Damit können auch vertrauliche Inhalte von Firmen etc. an Privat-Peronen per E-Mail geschickt werden.
- Jederzeit kann der Empfänger einen neuen Public Key und Private Key für alle neuen E-Mails erzeugen.