Praktikum: GnuPG auf der Kommandozeile

- Starte den Rechner (unter Linux) und öffne ein Terminal. Es öffnet sich ein Kommandozeilenterminal in welchem dem Computer Befehle gegeben werden können

Informationsquellen

- http://www.stierand-linuxit.de/Doku/gpg-tutorial.html (Knapp und pragmatisch)
- http://wiki.kairaven.de/open/krypto/gpg/gpganleitung (Sehr ausführlich mit vielen Hintergrundinfos)

Aufgaben

Fertige im Verlauf des Praktikums eine Liste aller verwendeten Befehle an. Liste die Befehle nicht nur auf, sondern beschreibe auch jeweils, was sie bewirken.

- Erzeuge ein Schlüsselpaar aus privatem und öffentlichem Schlüssel. Der private Schlüssel soll dabei durch ein Kennwort geschützt sein.
- Verschlüssle eine Textdatei. Eine Textdatei kannst du mit einem Editor erzeugen, den du im Dash findest, wenn du nach "Textbearbeitung" suchst. Warum wird beim Verschlüsseln nicht nach dem Passwort für den Schlüssel gefragt?

- Betrachte das Ergebnis der Verschlüsselung (sowohl als Binärdatei als auch als ASCII-Datei was musst du beachten, um eine ASCII-Datei zu erhalten?). [Ein Kommandozeilenprogramm zum ansehen von Dateien ist `less`. Du öffnest deine Datei mit dem Befehl `less [Dateiname]`, schließen kannst du die Ausgabe durch den Befehl `q`.
- Lasse dir alle öffentlichen und privaten Schlüssel anzeigen, die du in deinem Schlüsselbund hast.
- Tauscht über das Tauschverzeichnis öffentliche Schlüssel aus und fügt sie in euren Schlüsselbund hinzu.
- Überprüfe, ob der Import der öffentlichen Schlüssel geklappt hat.
- Verschlüsselt eine Nachricht an einen anderen Empfänger mit dessen öffentlichem Schlüssel, so dass der Empfänger die Datei aus dem Tauschlaufwerk holen kann und bei sich mit Hilfe seines privaten Schlüssels entschlüsseln kann
- Signiert eine Nachricht an einen Mitschüler, sowohl mit dem Kommandozeilenschalter `-s` also auch mit `--clearsign`.
- Überprüft die Signatur
- Versucht, eine mit `--clearsign` signierte Nachricht zu manipulieren und anschließend die Signatur zu überprüfen.
- Schicke eine verschlüsselte und signierte Nachricht an deinen Partner, entschlüssle die Nachricht deines Partners und verifiziere die Signatur.