Verschlüsseln von einzelnen Dateien mit GPG

- ## Variante 1: Symmetrisches Verfahren

verschlüsseln mit Standartwerten:
```
gpg -c DATEINAME.TXT
```

Das Passwort zum verschlüsseln muss 2x eingegeben werden.

entschlüsseln:
```
gpg -d DATEINAME.TXT.GPG > DATEINAME.TXT
```

Das Passwort zum entschlüsseln muss 1x eingegeben werden.

verschlüsseln mit anderem Algorithmus:
dazu müssen wir zuerst prüfen welche Verschlüsselungsalgorithmen auf unserem System Installiert sind.
```
gpg --version
```

Es kommt dann wahrscheinlich so was bei raus.
```
Verschlü.: IDEA, 3DES, CAST5, BLOWFISH, AES, AES192, AES256,
TWOFISH, CAMELLIA128, CAMELLIA192, CAMELLIA256
```

verschlüsseln mit z.B. AES256:
```
gpg --symmetric --cipher-algo AES256 DATEINAME.TXT
```

Das Passwort zum verschlüsseln muss 2x eingegeben werden.

entschlüsseln:
```
gpg -d DATEINAME.TXT.GPG > DATEINAME.TXT
```

Das Passwort zum entschlüsseln muss 1x eingegeben werden.

- ## Variante 2: Asymmetrisches Verfahren

verschlüsseln mit einem oder mehren öffentlichen Schlüsseln:
```
gpg -e DATEINAME.TXT
```

gib die 8-Stellige User-ID des entsprechenden Schlüssels ein oder ggf. die emailadresse.

entschlüsseln:
```
gpg -d DATEINAME.TXT.GPG > DATEINAME.TXT
```

Die Passphrase zum entschlüsseln muss 1x eingegeben werden.

Hinweis 1: gpg erstellt beim verschlüsseln und entschlüsseln jeweils eine Kopie, so das nach dem Verschlüsseln die Originaldatei immer noch unverschlüsselt auf dem Datenträger liegt.

Hinweis 2: über diese verfahren kann man jede Art von Datei auch .jpg, .wav, .odt, .pdf, etc. verschlüsseln.

Hinweis 3: verschlüsselte Dateien haben die Dateiendung .gpg.