Verschlüsseln von Dateien und E-Mails

Verschlüsseln mit ccrypt

Das Programm ccrypt kann direkt aus den Paketquellen installiert werden.

- Verschlüsseln:

```
ccencrypt foobar
```

- Entschlüsseln:

```
ccdecrypt foobar
```

- Entschlüsseln – nur auf die Standardausgabe:

```
ccat foobar
```

Weitere Informationen bietet die Manpage zur Anwendung.

GPG

Um ein Dokument zu verschlüsseln, benutzt man die Option `--encrypt`. Dazu müssen Sie die öffentlichen Schlüssel der vorgesehenen Empfänger haben. Sollten Sie auf der Kommandozeile den Namen der zu verschlüsselnden Datei nicht angeben, werden die zu verschlüsselnden Daten von der Standard-Eingabe gelesen. Das verschlüsselte Resultat wird auf die Standard-Ausgabe oder in die Datei, die durch die Option `--output` spezifiziert ist, geschrieben. Das Dokument wird darüberhinaus auch noch komprimiert.

```
alice$ gpg --output doc.gpg --encrypt --recipient blake@cyb.org doc
```

Mit der Option `--recipient` wird der öffentliche Schlüssel spezifiziert, mit dem das Dokument verschlüsselt werden soll. Entschlüsseln läßt sich das so verschlüsselte Dokument jedoch nur von jemandem mit dem dazugehörigen geheimen Schlüssel. Das bedeutet konsequenterweise aber auch, daß Sie selbst ein so verschlüsseltes Dokument nur wieder entschlüsseln können, wenn Sie Ihren eigenen öffentlichen Schlüssel in die Empfängerliste aufgenommen haben.

Zum Entschlüsseln einer Nachricht wird die Option `--decrypt` benutzt. Sie benötigen dazu den geheimen Schlüssel, für den die Nachricht verschlüsselt wurde und das Mantra, mit dem der geheime Schlüssel geschützt ist.

```
blake$ gpg --output doc --decrypt doc.gpg
Sie benötigen ein Mantra, um den geheimen Schlüssel zu entsperren.
Benutzer: ``Blake (Staatsanwalt) <blake@cyb.org>''
1024-Bit ELG-E Schlüssel, ID F251B862, erzeugt 2000-06-06 (Hauptschlüssel-ID B2690E6F)
```

Revision #1
Created 21 March 2023 08:05:04 by Hermann
Updated 21 March 2023 08:05:15 by Hermann