Encryptie

- Encryptie en decryptie met gpg

Encryptie en decryptie met gpg

Met behulp van de Linux tool gpg kan je bestanden versleutelen (encrypten) en ook weer ontsleutelen (decrypten).
De methode die we hier bespreken is "Symmetric Encryption". We versleutelen hierbij het bestand met een enkel wachtwoord (passphrase).

In Debian Linux kan je eerst controleren of gpg al geïnstalleerd is met:

```
gpg --version
```

Mocht dit nog niet het geval zijn, dan kan je gpg installeren met:

```
sudo apt install gnupg
```

Encryptie van bestanden

Je kunt een bestand versleutelen met de volgende opdracht. Hierbij geven we het versleutelwachtwoord op in de commandoregel:

```
gpg --batch -c --passphrase 'passphrase' file.txt
```

Veiliger is om het wachtwoord (passphrase) in een apart bestand te zetten en deze zodanig rechten te geven dat deze bijvoorbeeld enkel te lezen is door de root gebruiker. In onderstaand voorbeeld staat het wachtwoord in /etc/gpg/pass.txt

```
gpg --batch -c --passphrase-file /etc/gpg/pass.txt file.txt
```

Het versleutelde bestand krijgt automatisch de extensie .gpg, dus in ons voorbeeld file.txt.gpg

Decryptie van bestanden

Wanneer je het wachtwoord meegeeft in de commandline:

```
gpg --batch --output file.txt --passphrase 'passphrase' --decrypt file.txt.gpg
```

Met behulp van het wachtwoordbestand wordt dit:

```
gpg --batch --output file.txt --passphrase-file /etc/gpg/pass.txt --decrypt file.txt.gpg
```

Hierbij geeft de optie --output aan welke naam je het ontsleutelde bestand wilt geven, in dit voorbeeld file.txt

Decryptie van meerdere bestanden tegelijk

Onderstaand commando is handig wanneer je meerdere bestanden tegelijk wilt decrypten.
Het voordeel hiervan is dat je geen "output" file hoeft op te geven.
De bestandsnaam wordt dezelfde naam zonder de .gpg extensie.
Je kunt hiermee ook een enkel bestand decrypten door de wildcard aan te passen.

```
gpg --batch --passphrase-file /etc/gpg/pass.txt --decrypt-files *.gpg
```