

Diffie-Hellman Parameterdatei Bitgröße ermitteln

Auf Diffie-Hellman aufsetzende Cipher benötigen eine entsprechende Parameterdatei. Die Standardgröße beträgt 1024 bit. Die Empfehlung nach der Logjam-Attacke sind mind. 2048 bit, besser 4096 bit.

Die Parameterdatei wird folgendermaßen erstellt:

```
openssl dhparam -out dhparams.pem 4096
```

Aus der Datei läßt sich die Bitgröße nicht auf Anhieb herauslesen. Mit diesem Befehl lässt sich die Info darstellen:

```
openssl dhparam -inform PEM -in dhparams.pem -check -text
```

Revision #1

Created 30 April 2021 12:02:58 by magenbrot

Updated 17 July 2021 15:03:13 by magenbrot