Kontrollfragen: Rückblick zur Kryptographie

- Welches drei Ziele verfolgt die Kryptographie?
- Was ist das Kerckhoffsche Prinzip?
- Welche klassischen Verfahren kennst du? Welche Schwächen haben die Verfahren - wie kann man sie angreifen?
- Was ist der Unterschied zwischen symmetrischen und asymmetrischen Verfahren? Nenne jeweils Beispiele.
- Vollziehe das RSA Verfahren nach (RSA by Example)
- Welchen Zweck verfolgt der Diffie Hellman Schlüsselaustausch? Was bedeutet der Begriff „Perfect Forward Secrecy“?
- Was muss man ans Anwender tun, um GPG zu verwenden?