

- Schreiben Sie eine Software für die Ver- und Entschlüsselung mit dem Stromchiffre RC4.
- Nutzen Sie Ihre RC4-Software für einen Brute-Force-Angriff auf den Chiffrattext. Starten Sie hierfür mit den Annahmen, dass (i) der Schlüsselraum klein ist und (ii) alle verwendeten Schlüsselbytes Kleinbuchstaben (ASCII-Code) sind. Gehen Sie auch diesmal wieder davon aus, dass der Klartext ein Text einer natürlichen Sprache ist.