Prof. Dr.-Ing. Kerstin Lemke-Rust Hochschule Bonn-Rhein-Sieg

Computerpraktikum: Aufgabenblatt 3

- **C.1** Implementieren Sie das LFSR mit dem primitiven Polynom $x^{21} + x^2 + 1$ in Software.

 - (b) Prüfen Sie durch Ausgabe des internen Zustands des LFSRs, dass die maximale Periode eines LFSRs bei diesem Polynom erreicht wird.
- C.2 Das Chiffrat encrypted.bin (Binärdatei) ist mit RC4 verschlüsselt worden, der Schlüssel ist unbekannt. Ihre Aufgabe ist es, den Klartext wiederzugewinnen. Gehen Sie dafür wie folgt vor:
 - (a) Schreiben Sie eine Software für die Ver- und Entschlüsselung mit dem Stromchiffre RC4.
 - (b) 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.