Angewandte Kryptographie 1 Prof. Dr.-Ing. Kerstin Lemke-Rust
SoSe 2023 Hochschule Bonn-Rhein-Sieg

Computerpraktikum: Aufgabenblatt 3

C.1 Implementieren Sie das LFSR mit dem primitiven Polynom $x^{17}+x^6+1$ in Software.

(a) Testen Sie Ihre Implementierung auf Korrektheit: Beim Initialisieren des LFSRs mit dem Wert 0x1FFFF sollten die folgenden ersten 64 Bits als Ausgabe des LFSRs sich ergeben:
`1111111111111111000000111111000001000000111110111100111101000000`

(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 Großbuchstaben (ASCII-Code) sind. Gehen Sie auch diesmal wieder davon aus, dass der Klartext ein Text einer natürlichen Sprache ist.