Angewandte Kryptographie
SoSe 2024

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

Computerpraktikum: Aufgabenblatt 2

C.1 Alice und Bob haben für ihre vertrauliche Kommunikation ein One-Time-Pad eingerichtet. Teile des von ihnen verwendeten One-Time-Pad Schüsselstroms sind jetzt jedoch kompromittiert worden. Entschlüsseln Sie das kürzlich aufgezeichnete Chiffrat chiffrat.bin unter Nutzung des Schlüsselstroms stream.dat (jeweils in LEA).

C.2 Zufallszahlengeneratoren sind in der Kryptographie ein sehr sensibles Thema, so insbesondere auch beim One-Time Pad.

Untersuchen Sie die statistischen Eigenschaften von drei verschiedenen Zufallszahlengeneratoren. Hierfür liegt von jedem Zufallszahlengenerator eine erzeugte Testdatei mit generierten Zufallszahlen vor.

(a) Welche statistischen Eigenschaften (z.B. Häufigkeitsverteilungen) und ggf. welche Schwachstellen (z.B. statistische "Schiefe", Periodizität) sind für den

i. Zufallszahlengenerator aus Aufgabe **C.1** (Test-Binärdatei stream.dat),
ii. Zufallszahlengenerator 1 (Test-Binärdatei stream1.dat) und
iii. Zufallszahlengenerator 2 (Test-Binärdatei stream2.dat)

jeweils nachweisbar?

(b) Ausgehend von möglichen Schwachstellen aus (a): Welche Entropie hat ein 128-Bit Schlüssel, der mit dem

i. Zufallszahlengenerator aus Aufgabe **C.1**,
ii. Zufallszahlengenerator 1 und
iii. Zufallszahlengenerator 2

erzeugt wurde?

Hinweise:

- Eine Sichtung der Inhalte der Binärdateien mit einem Hexdump-Tool (z.B. hexdump unter Linux) ist für diese Aufgabe hilfreich.