Überblick Mittwoch

- Structs, Aufgabe 4 (fertig)
- Kryptographie (Demo: Revil)
- Aufgabe 5 und 6
- Kompression (Demo: APLib)
- Aufgaben 7

Aufgabe 4 (Teil 2 und 3)

https://mal.re/tmp/classes/hsbund-ws2026/tag2/aufgabe4.md

Kryptographie & Kompression

- Strings wie "unzip 0.15 Copyright 1998..."
- Viel Arithmetik: +, *, <<, |
- Charakteristische Konstanten

Kryptographie

- Großer und kleiner Puffer (Ciphertext & Key)
- Charakteristische Konstanten (Block Cipher)
- S-Boxen
- Stream Cipher sind schwer (wir zeigen häufige)
- Asymmetrische Crypto lassen wir aus

Sehr beliebte Stream-Cipher

- Salsa ("expand 32-byte k")
- RC4 (256 byte S-Box, Loop, Loop)
- RC4 never forget!

Demo: REvil

Block-Cipher

- AES (Awesome Encryption Standard)
- DES/DES3 (Data Encryption Standard)
- TEA (Tiny Encryption Algorithm)

Easy Wins (Signaturen)

- S-Box (AES, DES)
- Nothing-up-my-sleeve number
  (TEA, Salsa20, CRC32, ...)

Aufgabe 5

https://mal.re/tmp/classes/hsbund-ws2026/tag3/aufgabe5.md

Aufgabe 6

https://mal.re/tmp/classes/hsbund-ws2026/tag3/aufgabe6.md

Kompression

- Kein Schlüssel
- Backrefs (negative offsets in Arrays)
- "Workbench" Puffer

Aufgabe 7

https://mal.re/tmp/classes/hsbund-ws2026/tag3/aufgabe7.md