Implementation of a Rainbow Table Attack

Cybersecurity
Prof. Dr. rer. nat. habil. Clemens H. Cap

Team:

Jasper Roloff
Alexander Saraev
Ovais Idrees
Marvin Davieds
Max Kaseler
Alexandra Plein
Bilal Shah

Current status

- Reduction function implementation
- Native python lib for SHA
- Data structure for rainbow table (may be changed)
- Our plaintext space: 208,000,000,000 (26^8)

Example calculation for 45 min target time:

- 4 CPU cores, per core:
  - chain length: 100,000
  - number of chains: 18,000

Next steps

- test runs
- efficient use of memory
- evaluate results with different k (hash length)