Hochschule für Technik und Wirtschaft
Studiengang Kommunikationsinformatik
Prof. Dr.–Ing. Damian Weber

Angewandte Kryptographie – Übung 5

Aufgabe 1 (Pollard–ϱ)

Implementieren Sie die Pollard–ϱ Methode (Floyd's Zykelfinder) um Kollisionen auf einem Teil des Outputs der Hashfunktion SHA–1 zu finden.

D.h. Ihr Programm soll Werte x, x' finden, für die die Hashwerte SHA1(x), SHA1(x') auf den unteren

- 32 Bits
- 64 Bits
- 96 Bits
- ... (oder mehr Bits?)

übereinstimmen. Je mehr desto besser.

Eine Klasse für SHA–1 finden Sie ebenfalls unter

`http://www-crypto.htw-saarland.de/weber/teaching/03_ws_ak/`