Studiengang Informatik
apsi 2021

Fachhochschule Nordwestschweiz
Arno Wagner, Michael Schläpfer

Übungsblatt 4 — 11. Oktober 2020

Aufgabe 4-1: Entropie

In der Vorlesung haben Sie gesehen, wie sich informationstheoretische Entropie berechnen lässt. Gehen Sie jetzt von einer Quelle aus, die 256 Zeichen mit Gleichverteilung erzeugt.

(a) Berechnen Sie die Entropie pro Zeichen.

(b) Wie würde sich die Entropie bei einer anderen Verteilung verhalten? Sinkt oder steigt die Entropie wenn glsichverteilung nicht mehr gegeben ist?

(c) Warum ist eine hohe Entropie so wichtig für kryptographische Anwendungen?

Aufgabe 4-2: Applied Cryptography am Beispiel von C

Lesen Sie die referenzierte Webseite und machen Sie sich mit einigen der Herausforderungen bei der Anwendung von Kryptographie vertraut:

`https://web.archive.org/web/20160525230135/https://cryptocoding.net/index.php/Coding_rules`

Aufgabe 4-3: Die vier Reiter der Infokalypse

Lesen Sie den nachfolgenden Link durch. Welche Problematik zeigt sich hier?

`https://en.wikipedia.org/wiki/Four_Horsemen_of_the_Infocalypse`