Studiengang Informatik
apsi 2020

Fachhochschule Nordwestschweiz
Arno Wagner, Michael Schläpfer, Rolf Wagner

Übungsblatt 4 — 5. Oktober 2020

Aufgabe 4-1: Entropie

In der Vorlesung haben Sie gesehen, wie sich die Entropie im informationstheoretischen Sinne berechnen lässt. Nehmen wir an, dass im Gegensatz zum Beispiel in der Vorlesung, die Quelle nun doppelt so viele Zeichen, nämlich 256, mit gleicher Wahrscheinlichkeit erzeugt.

(a) Berechnen Sie die Entropie pro Zeichen.

(b) Wie würde sich die Entropie verhalten, bei einer anderen Verteilung, d.h. wenn einzelne Zeichen eine höhere Auftretenswahrscheinlichkeit hätten?

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

Aufgabe 4-2: Applied Cryptography am Beispiel von C

Lesen Sie die nachfolgende Webseite und machen Sie sich mit den Herausforderungen in 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`