Studiengang Informatik **Fachhochschule Nordwestschweiz**
apsi 2019 Arno Wagner, Michael Schläpfer

Lösungsblatt 5 21. Oktober 2019

Aufgabe 5-1: Entropie

(a) Analog zum Beispiel in der Vorlesung berechnen wir

$$E = -\sum_{i=0}^{n-1} p_i * log_2(p_i)\ bit$$

mit 256 Symbolen, die alle gleich wahrscheinlich auftreten ergibt sich also folgende Berechnung für E:

$$E = -\sum_{i=0}^{255} \frac{1}{256} * log_2(\frac{1}{256})\ bit$$

also,

$$E = -log_2(\frac{1}{256}) = 8\ bit$$

(b) Nehmen wir folgendes vereinfachtes Beispiel anhand eines Münzwurfs. Bei einer fairen Münze ist die Entropie

$$E = -log_2(\frac{1}{2}) = 1\ bit$$

Vergleichen wir dies nun mit einer unfairen Münze, bei der Kopf mit einer Wahrscheinlichkeit von $p = \frac{3}{4}$ auftritt. Damit ergibt sich folgende Entropie:

$$E = -\left[\frac{3}{4} * log_2(\frac{3}{4}) + \frac{1}{4} * log_2(\frac{1}{4})\right] \sim 0.8\ bit$$

Das Ergebnis eines unfairen Münzwurfes ist also vorhersehbarer und weniger überraschend. Demnach ist auch der Informationsgehalt tiefer. Was mit der Intuition übereinstimmt.

(c) Kryptographische Protokolle basieren auf Zufallszahlen, beispielsweise für die Erstellung von Schlüsseln um eine Verbindung abzusichern, etc. Sind diese Zufallszahlen vorhersehbar für einen Angreifer, kann er die kryptographischen Funktionen nachvollziehen und deren Schutz umgehen. Werden beispielsweise gleich nach einem Systemstart, wenn noch wenig Entropie zur Verfügung steht, Schlüssel generiert, so stellen diese unter Umständen Schlüssel aus einer kleinen Menge möglicher Schlüssel dar und dies unabhängig von der Länge der Schlüssel selbst.

Aufgabe 5-2: Applied Cryptography am Beispiel von C

Der Link gibt Aufschluss über einige der Herausforderungen, welche sich im Zusammenhang mit Kryptographie stellen.

Aufgabe 5-3: Die vier Reiter der Infokalypse

Der Angegebene Link zeigt auf, dass jederzeit damit gerechnet werden muss, dass gespeicherte Daten zur Verfügung gestellt werden müssen. Entsprechend gilt der in der Vorlesung getätigte Ratschlag, wonach möglichst nur diejenigen Daten gespeichert werden sollten, die für die Anwendung wirklich nötig sind. Alle anderen sollten wenigsten anonymisiert werden.