Dr. Dirk Frettlöh 6.5.2020

# Übungen zur Vorlesung Kryptographie

## Blatt 5

**Aufgabe 17: (Zufall)**
Ein Zufallsgenerator mit Werten in $\{1, 2, \ldots, n\}$ heißt *fair*, wenn jedes Ergebnis gleich wahrscheinlich ist. Werfen einer normalen Münze ist fair (2 Werte); das Werfen eines gewöhnlichen Spielwürfels (6 Werte) auch.

**(a)** Erfinden Sie einen fairen 17seitigen Spielwürfel.
**(b)** Sie bekommen eine beliebig lange 0-1-Sequenz, die mit einer unfairen Münze erzeugt wurde (z.B. viel mehr 0en als 1en). Wie können Sie daraus eine Sequenz ableiten, die von der mit einer fairen Münze erzeugten nicht zu unterscheiden ist?
**(c)** Wie lange müssen Sie im Schnitt mit einem fairen gewöhnlichen Spielwürfel würfeln, bis eine 6 kommt? *(Begründen Sie Ihre Antwort, Sie dürfen den Grund aber auch googeln.)*

**Aufgabe 18: (Topologische Entropie)**
Berechnen Sie die topologische Entropie der folgenden unendlichen (besser: zweiseitig unendlichen) Worte $w = \cdots w_{-2}w_{-1}w_0w_1w_2\cdots$

**(a)** $w = \cdots 111111000000\cdots$, wobei $w_i \in \{0, 1\}$. Also $w_i = 1$, falls $i < 0$, $w_i = 0$ falls $i \geq 0$.
**(b)** $w = \cdots 0w_{-2}0w_00w_20w_4\cdots$, mit $w_i \in \{0, 1, 2, 3\}$, wobei $w_i = 0$, falls $i$ ungerade, $w_i$ zufällig 0, 1, 2 oder 3, mit Wahrscheinlichkeit jeweils $\frac{1}{4}$ (und unabhängig von den anderen $w_j$) falls $i$ gerade.
**(c*)** $w = \cdots w_{-2}w_{-1}w_0w_1w_2\cdots$ mit $w_i \in \{0, 1\}$, und $w$ hat die Eigenschaft, dass es keine benachbarten Einsen enthält.

> (b) und (c) sind "fast alle"-Aussagen: fast alle diese Worte haben dieselbe Entropie $h(w)$. Das Wort $\cdots 00000\cdots$ z.B. ist eine Ausnahme: es hat auch die jeweils geforderte Eigenschaft, hat aber Entropie 0. Fast alle Worte mit der jeweiligen Eigenschaft enthalten aber alle erlaubten Teilworte der Länge $m$, und haben eine positive Entropie. Diese soll berechnet werden.

**Aufgabe 19: (Pseudo-Zufall vorhersagen)**
Sie belauschen die folgende Sequenz von Pseudozufallszahlen: $13, 223, 793, 483, 213, 623, 593, \ldots$. Sie wissen, dass diese durch einen Linearen Kongruenzgenerator $x_i = sx_{i-1} + t \mod m$ erzeugt wurde. Finden Sie passende Werte für $s, t$ und $m$, und geben Sie einen guten Tipp für die nächste Pseudozufallszahl ab.

*Sie können sich gerne selbst etwas ausdenken (raten ist OK!), aber hier steht auch eine Anleitung:*

`https://www.math.uni-bielefeld.de/~frettloe/teach/krypto/lc-prng.png`

*Aufgabe 20 auf der nächsten Seite.*

**Aufgabe 20 (Topologische Shannon-Entropie)**
Eines der folgenden 0-1-Worte (Länge 256) habe ich mir ausgedacht, eines ist mit einem Pseudo-Zufallsgenerator erzeugt worden.

Wort 1:

1, 0, 1, 0, 0, 1, 1, 1, 0, 0, 1, 0, 1, 0, 0, 0, 0, 1, 1, 1, 1, 0, 1, 0, 1, 0, 1, 1, 1, 1, 0, 0, 1, 0, 0, 1, 1, 1, 0, 0, 1, 1, 1, 1, 0,
0, 1, 1, 0, 1, 0, 1, 1, 1, 1, 0, 0, 0, 1, 1, 0, 0, 1, 1, 0, 1, 0, 1, 1, 0, 0, 0, 0, 0, 1, 0, 1, 1, 0, 1, 0, 0, 1, 0, 1, 0, 0, 1, 1, 1,
0, 1, 0, 1, 0, 0, 1, 1, 1, 1, 0, 0, 0, 0, 1, 1, 1, 1, 0, 1, 0, 0, 0, 0, 0, 0, 0, 1, 0, 0, 0, 1, 0, 1, 0, 0, 0, 0, 0, 0, 1, 0, 1, 1, 0,
0, 1, 1, 1, 0, 1, 0, 0, 1, 0, 0, 1, 0, 0, 0, 1, 1, 0, 0, 1, 1, 1, 1, 1, 0, 0, 0, 0, 1, 1, 1, 1, 1, 1, 0, 1, 0, 0, 0, 1, 0, 1, 1, 1, 1,
0, 1, 1, 0, 0, 0, 1, 0, 1, 0, 1, 1, 0, 0, 0, 1, 0, 0, 1, 1, 1, 0, 1, 0, 1, 1, 0, 0, 0, 1, 0, 0, 1, 0, 0, 0, 1, 1, 1, 0, 1, 1, 1, 0, 0,
0, 0, 0, 1, 0, 0, 1, 0, 1, 1, 0, 1, 1, 1, 0, 0, 1, 0, 0, 1, 1, 1, 0, 1, 1, 0, 0, 0, 1, 1, 1.

Wort 2:

1, 0, 1, 1, 1, 0, 0, 1, 1, 1, 0, 0, 0, 1, 0, 0, 1, 0, 1, 0, 1, 1, 0, 1, 1, 0, 0, 0, 1, 0, 1, 1, 1, 0, 0, 1, 0, 1, 0, 1, 1, 1, 0, 0, 1,
0, 0, 0, 1, 0, 1, 0, 1, 0, 0, 0, 1, 0, 1, 1, 1, 0, 1, 1, 0, 0, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 1, 0, 1, 1, 0, 0, 0, 0, 0, 1, 0, 1, 0, 1,
1, 0, 1, 0, 0, 1, 0, 1, 0, 0, 1, 1, 1, 1, 0, 1, 0, 1, 1, 0, 0, 0, 1, 0, 1, 0, 1, 1, 1, 0, 1, 0, 1, 1, 1, 0, 1, 0, 1, 0, 0, 0, 1, 1, 1,
0, 1, 0, 0, 0, 0, 1, 0, 1, 1, 1, 0, 1, 0, 1, 1, 1, 1, 0, 1, 0, 1, 1, 0, 1, 0, 1, 1, 0, 1, 1, 0, 1, 1, 0, 1, 0, 0, 1, 0, 0, 0, 0, 1, 1,
1, 0, 1, 1, 0, 1, 0, 0, 0, 1, 0, 1, 1, 0, 1, 1, 1, 0, 1, 0, 1, 1, 0, 1, 1, 0, 0, 1, 0, 1, 0, 1, 0, 0, 0, 1, 0, 0, 1, 1, 1, 0, 1, 0, 1,
0, 1, 0, 1, 1, 1, 0, 1, 1, 0, 1, 0, 0, 0, 1, 0, 1, 1, 1, 1, 0, 1, 0, 1, 1, 1, 1, 0, 1, 0, 1.

Finden Sie heraus, welches das ausgedachte Wort ist. Benutzen Sie dazu eine Kombination von Shannon-Entropie („ausgewogene Häufigkeit") und topologischer Entropie („Zählen der verschiedenen Teilworte"). Gehen Sie dazu so vor:

Ein Teilwort der Länge $k$ eines Wortes $w_1 w_2 \cdots w_m$ ist ein Wort $w_{i+1} \cdots w_{i+k}$ ($0 \leq i \leq m-k$). Erstellen Sie eine Liste $m_0, m_1, \ldots, m_{15}$ mit den jeweiligen Häufigkeiten der möglichen Teilworte der Länge 4 in Wort 1, und eine entsprechende Liste $k_0, k_1, \ldots, k_{15}$ für Wort 2. (Beispiel: ein mögliches Teilwort ist 0000. Das kommt 4mal in Wort 2 vor, also $k_0 = 4$. Obacht: kommt einmal z.B. 00000 vor, zählt das als zweimaliges Auftauchen von 0000.)

Berechnen Sie dann dazu jeweils die Shannon-Entropie $H(w)$ in der angepassten Variante mit $P_i = \frac{1}{253} m_i$, bzw. $P_i = \frac{1}{253} k_i$. (Dabei ist in der Formel für $H$ das $b = 16$.) Angenommen, ich bin kein guter Zufallsgenerator: Welches der Worte habe ich mir ausgedacht?

---

Abgabe bis Mittwoch 13.5.2020 bis 14 Uhr per Email an den Tutor.

Philipp Braukmann pbraukmann@techfak.de
Jonas Friemel jfriemel+krypto@techfak.de