

Übungen zur Vorlesung Kryptographie

Blatt 5

Aufgabe 17: (Spielzeugbeispiel für Shannon-Entropie)

(a) Berechnen Sie von Hand die Shannonentropie $H(w)$ der folgenden drei Worte $w = w_1w_2 \cdots w_{16}$, wobei die w_i aus dem Alphabet $\{0, 1, 2, 3\}$ (!) sind.

1011031331011031 3131131131333113 2310111312311031.

(b) (*Knifflig:*) Zeigen Sie: wenn das Alphabet b Buchstaben hat, dann wird die maximale Shannon-Entropie $H(w) = 1$ nur erreicht bei $P_i = \frac{1}{b}$ für $i = 1, \dots, b$.

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) $w = \cdots 000000111111 \cdots$, 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 also für i ungerade i gilt: $w_i = 0$; und für gerade i gilt: w_i zufällig 0, 1, 2 oder 3, mit Wahrscheinlichkeit jeweils $\frac{1}{4}$ (und unabhängig von den anderen w_j).

(c) $w = \cdots w_{-2}w_{-1}w_0w_1w_2 \cdots$ mit $w_i \in \{0, 1, 2, 3\}$, und w hat die Eigenschaft, dass keine benachbarten Zahlen w_i gleich sind. Also gilt: $w_i \neq w_{i+1}$ für alle $i \in \mathbb{Z}$.

(b) und (c) sind "fast alle"-Aussagen: fast alle diese Worte haben dieselbe Entropie $h(w)$. Das Wort $\cdots 010101010 \cdots$ 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: (Lineare Kongruenz-PRNGs)

Wir betrachten lineare Kongruenzgeneratoren mit $x_{i+1} \equiv s \cdot x_i + t \pmod{N}$ (vergleiche Skript).

(a) Berechnen Sie die Pseudozufallszahlensequenzen x_0, x_1, x_2, \dots für

- | | |
|--------------------------------------|--------------------------------------|
| (1) $N = 12, s = 2, t = 3, x_0 = 4.$ | (2) $N = 12, s = 4, t = 2, x_0 = 1.$ |
| (3) $N = 13, s = 2, t = 3, x_0 = 4.$ | (4) $N = 13, s = 4, t = 2, x_0 = 1.$ |

(b) In (a) fällt auf, dass die Periodenlängen der erzeugten Sequenzen Teiler von $\varphi(12) = 4$ (in (1) und (2)) bzw von $\varphi(13) = 12$ (in (3) und (4)) sind. Tatsächlich gilt:

In einer von einem linearen Kongruenzgenerator mit Parameter N erzeugten Sequenz x_0, x_1, \dots wiederholen sich die Elemente immer nach $\varphi(N)$ Schritten.

Beweisen Sie diese Aussage für $s \in \mathbb{Z}_N^*$ und $s - 1 \in \mathbb{Z}_N^*$.

Aufgabe 20 auf der nächsten Seite.

Aufgabe 20 (Topologische Entropie anwenden)

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

Wort 1:

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

Wort 2:

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

Finden Sie heraus, welches das ausgedachte Wort ist. Benutzen Sie dazu die topologische Entropie („Zählen der verschiedenen Teilworte“). Gehen Sie dazu so vor:

Ein Teilwort der Länge k eines Wortes $w_1w_2 \cdots w_m$ ist ein Wort $w_{i+1} \cdots w_{i+k}$ ($0 \leq i \leq m - k$). Erstellen Sie eine Liste mit den allen Teilworten der Länge 6 in Wort 1, und eine entsprechende Liste für Wort 2. Angenommen, ich bin kein guter Zufallsgenerator: Welches der Worte habe ich mir ausgedacht? Und wie kommen sie darauf?

Abgabe bis Mittwoch 20.5.2026 bis 12:00 Uhr per Email an die Tutorin.

Lisa Henetmayr Mi 12 Uhr in S0-115 lhenetmayr+krypto@techfak.de
Lisa Henetmayr Mi 16 Uhr in U2-147 lhenetmayr+krypto@techfak.de