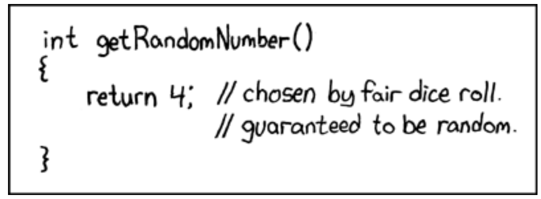
Dr. Dirk Frettlöh 9.5.2022

Übungen zur Vorlesung Kryptographie

Blatt 5



Quelle xkcd.com

Aufgabe 17: (Spielzeugbeispiel für Shannon-Entropie)
(a) Berechnen Sie von Hand die Shannonentropie $H(w)$ der folgenden drei Worte $w = w_1 w_2 \cdots w_{16}$, wobei die w_i aus dem Alphabet $\{0,1,2,3\}$ sind.

$$1113301001311310 \qquad 1131131331333113 \qquad 0312131110311231.$$

(b) Zeigen Sie: wenn das Alphabet n Buchstaben hat, aber in dem Wort w nur $k < n$ verschiedene Buchstaben vorkommen, dann gilt $H(w) \le \frac{k}{n}$.

Aufgabe 18: (Topologische Entropie)
Berechnen Sie die topologische Entropie der folgenden unendlichen (besser: zweiseitig unendlichen) Worte $w = \cdots w_{-2} w_{-1} w_0 w_1 w_2 \cdots$

(a) $w = \cdots 000000111111 \cdots$, wobei $w_i \in \{0,1\}$. Also $w_i = 1$, falls $i < 0$, $w_i = 0$ falls $i \ge 0$.
(b) $w = \cdots 0 w_{-2} 0 w_0 0 w_2 0 w_4 \cdots$, 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) $w = \cdots w_{-3} w_{-2} w_{-1} w_0 w_1 w_2 w_3 w_4 \cdots$, mit $w_i \in \{0,1,2,3\}$, wobei für i ungerade gilt: w_i zufällig 0 oder 2 (mit Wahrscheinlichkeit $\frac{1}{2}$), und für i gerade gilt: w_i zufällig 1 oder 3 (mit Wahrscheinlichkeit $\frac{1}{2}$, und unabhängig von den anderen w_j)

(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 $x_{i+1} \equiv s \cdot x_i + t \bmod N$ (vergleiche Skript).

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

(1) $N = 12, s = 3, t = 3, x_0 = 3.$ (2) $N = 12, s = 5, t = 3, x_0 = 3.$
(3) $N = 13, s = 2, t = 3, x_0 = 3.$ (4) $N = 13, s = 3, t = 3, x_0 = 3.$

(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 $x_0, x_1, \ldots$ widerholen sich die Elemente immer nach $\varphi(N)$ Schritten.

Beweisen Sie diese Aussage, falls $s \in Z_N^* \setminus \{1\}$ ist.

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:

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

Wort 2:

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

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 $w_1 w_2 \cdots w_m$ ist ein Wort $w_{i+1} \cdots w_{i+k}$ $(0 \leq i \leq m-k)$. Erstellen Sie eine Liste 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 Montag 16.5.2022 bis 14 Uhr per Email an Ihren Tutor.
Bitte auf jeder Abgabe das Tutorium angeben. Bitte die Abgaben so nennen:
techfakaccount-bl$n$.pdf, also z.B. `dfrettloeh-bl5.pdf`, oder `dfrettloeh+mnebel-bl5.pdf`.

Jan-Philipp Brünger	jbruenger@techfak.de
Simon Hahm	shahm+krypto@techfak.de
Tim Lakämper	tlakaemper+krypto@techfak.de