Dr. Dirk Frettlöh 15.5.2019

Übungen zur Vorlesung Kryptographie

Blatt 6

Aufgabe 21: (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) $w = \cdots 11101110111011101110\cdots$, wobei $w_i \in \{0,1\}$. Also $w_i = 0$, falls $i \equiv 0 \bmod 4$, $w_i = 1$ sonst.
(b) $w = \cdots 111111000000\cdots$, wobei $w_i \in \{0,1\}$. Also $w_i = 1$, falls $i < 0$, $w_i = 0$ falls $i \geq 0$.
(c) $w = \cdots 0w_{-2}0w_00w_20w_4\cdots$, 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.

Aufgabe 22: (Mehr topologische Entropie)
Sei $w = \cdots w_{-2}w_{-1}w_0w_1w_2\cdots$ ein unendliches Wort mit der Eigenschaft, dass es keine benachbarten Einsen enthält. Berechnen Sie die topologische Entropie eines solchen Wortes.

A 21 (c) und A 22 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 23: (Schlechte Saat)
Manche Startwerte sind für einen Linearen Kongruenzgenerator ungeeignet.

(a) Gegeben ein Linearer Kongruenzgenerator (s. Skript) mit $m = 13, s = 3, t = 7$. Bestimmen Sie alle Startwerte x_0 so dass gilt: $x_{i+1} = x_i$ für alle $i \geq 0$.
(b) Machen Sie das gleiche wie in (a) für $m = 13, s = 7, t = 11$.
(c) Gegeben ein Linearer Kongruenzgenerator mit irgendwelchen m, s, t. Bestimmen Sie, für wieviele Startwerte x_0 gilt: $x_{i+1} = x_i$ für alle $i \geq 0$.

Aufgabe 24*: (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`

Abgabe: Mittwoch 22.5.2019 bis 14 Uhr in Postfach 2183 in V3, oder per Email an den Tutor.
Bitte auf jeder Abgabe das Tutorium angeben! (Di oder Do)

Dienstag	Philipp Braukmann	pbraukmann@techfak.uni-bielefeld.de
Donnerstag	Oliver Tautz	otautz@techfak.uni-bielefeld.de