

Übungen zur Vorlesung Kryptographie

Blatt 5

```

int getRandomNumber()
{
    return 4; // chosen by fair dice roll.
              // guaranteed to be random.
}

```

Quelle xkcd.com

Aufgabe 17: (Spielzeugbeispiel für Shannon-Entropie)

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

1123302001321320 1130101331010113 2222333322223333, 0132313330133213.

Aufgabe 18: (Topologische Entropie)

Berechnen Sie die topologische Entropie der folgenden unendlichen Worte $w = w_0w_1w_2 \cdots$.

(a) $w = 012301230123012301230 \cdots$ (also $w_i = i \bmod 4$).

(b) $w = 0w_20w_40w_60 \cdots$, wobei $w_i = 0$, falls i ungerade; und 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*) $w = w_0w_1w_2 \cdots$ mit $w_i \in \{0, 1\}$, wobei $w_i = 1$, falls i eine Zweierpotenz ist, und $w_i = 0$, falls i keine Zweierpotenz ist.

(b) ist eine “fast alle”-Aussage: fast alle diese Worte haben dieselbe Entropie $h(w)$. Das Wort 00000... z.B. ist eine Ausnahme: es hat auch die 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.

(c) ist ziemlich knifflig, es gibt auch schon Punkte, wenn Sie eine nicht-triviale obere oder untere Schranke finden, oder ihre Antwort richtig ist, aber nur plausibel hergeleitet anstatt perfekt bewiesen.

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 $x_0, x_1, x_2, \dots$ für

(1) $N = 10, s = 3, t = 2, x_0 = 2$. (2) $N = 10, s = 4, t = 3, x_0 = 2$.

(3) $N = 13, s = 3, t = 4, x_0 = 3$. (4) $N = 13, s = 4, t = 3, x_0 = 3$.

(b) In (a) fällt auf, dass die Periodenlängen der erzeugten Sequenzen Teiler von $\varphi(10) = 4$ (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 (ab irgendeinem x_i , nicht unbedingt ab x_0). Beweisen Sie diese Aussage, falls $s \in \mathbb{Z}_N^* \setminus \{1\}$ ist.

Aufgabe 20 (Reales Beispiel für Shannon-Entropie)

Eine der beiden Listen auf der folgenden Seite ist ein deutscher Text (mit der gewohnten Codierung a=0, b=1, ..., z=25), der andere ist zufällig erzeugt (strenggenommen pseudozufällig mit der `random`-Funktion von `python` bzw. `sagemath`). Berechnen Sie die Shannonentropie von beiden. Welches ist der deutsche Text? (Zusatzfrage ohne Punkte: wer schrieb ihn)?

13, 20, 13, 17, 4, 8, 18, 19, 3, 20, 0, 11, 18, 14, 25, 20, 12, 4, 17, 18, 19, 4, 13, 12, 0, 11, 8, 13, 3, 4, 8, 13, 4, 12, 11, 4, 1, 4, 13, 13, 0, 2, 7, 16, 20, 0, 11, 8, 19, 24, 11, 0, 13, 3, 1, 8, 18, 19, 3, 20, 18, 2, 7, 14, 13, 0, 20, 5, 6, 4, 17, 4, 6, 19, 9, 0, 0, 20, 18, 6, 20, 19, 4, 12, 6, 17, 20, 13, 3, 3, 4, 13, 13, 1, 0, 11, 3, 1, 4, 19, 17, 8, 19, 19, 18, 19, 3, 20, 3, 0, 18, 11, 0, 13, 3, 3, 0, 18, 18, 14, 22, 8, 2, 7, 19, 8, 6, 8, 18, 19, 3, 0, 18, 18, 12, 8, 19, 18, 4, 8, 13, 4, 17, 6, 17, 20, 4, 13, 3, 20, 13, 6, 4, 8, 13, 4, 13, 4, 20, 4, 25, 4, 8, 19, 17, 4, 2, 7, 13, 20, 13, 6, 1, 4, 6, 0, 13, 13, 3, 8, 4, 16, 20, 0, 11, 8, 19, 24, 19, 8, 12, 4, 3, 0, 3, 20, 3, 8, 2, 7, 8, 13, 16, 20, 0, 11, 8, 19, 24, 11, 0, 13, 3, 13, 14, 2, 7, 13, 8, 2, 7, 19, 0, 20, 18, 10, 4, 13, 13, 18, 19, 7, 0, 1, 4, 13, 22, 8, 17, 3, 8, 17, 7, 8, 4, 17, 4, 8, 13, 15, 0, 0, 17, 4, 8, 13, 11, 4, 8, 19, 4, 13, 3, 4, 8, 13, 5, 14, 17, 12, 0, 19, 8, 14, 13, 4, 13, 25, 20, 18, 0, 12, 12, 4, 13, 6, 4, 18, 19, 4, 11, 11, 19, 25, 22, 4, 8, 9, 0, 7, 17, 4, 21, 14, 17, 3, 4, 17, 6, 17, 20, 4, 13, 3, 20, 13, 6, 21, 14, 13, 16, 20, 0, 11, 8, 19, 24, 11, 0, 13, 3, 25, 22, 4, 8, 9, 0, 7, 17, 4, 21, 14, 17, 16, 20, 0, 11, 8, 19, 24, 19, 8, 12, 4, 0, 11, 18, 14, 6, 0, 1, 4, 18, 4, 8, 13, 4, 14, 4, 10, 14, 13, 14, 12, 8, 18, 2, 7, 4, 10, 17, 8, 18, 4, 18, 14, 11, 2, 7, 4, 13, 0, 20, 18, 12, 0, 18, 18, 4, 18, 3, 0, 18, 18, 3, 8, 4, 12, 4, 13, 18, 2, 7, 4, 13, 18, 8, 4, 0, 11, 18, 9, 0, 7, 17, 7, 20, 13, 3, 4, 17, 19, 10, 17, 8, 18, 4, 1, 4, 25, 4, 8, 2, 7, 13, 4, 19, 4, 13, 4, 18, 22, 0, 17, 1, 4, 17, 4, 8, 19, 18, 3, 8, 4, 3, 17, 8, 19, 19, 4, 9, 0, 7, 17, 7, 20, 13, 3, 4, 17, 19, 10, 17, 8, 18, 4, 8, 13, 13, 4, 17, 7, 0, 11, 1, 4, 8, 13, 4, 17, 3, 4, 10, 0, 3, 4, 21, 14, 13, 3, 4, 17, 15, 0, 13, 8, 10, 3, 4, 17, 12, 0, 4, 17, 10, 19, 4, 12, 8, 19, 6, 4, 17, 8, 18, 18, 4, 13, 1, 0, 19, 3, 8, 4, 17, 4, 6, 8, 4, 17, 20, 13, 6, 3, 8, 4, 20, 13, 19, 4, 17, 13, 4, 7, 12, 4, 13, 18, 1, 4, 17, 0, 19, 4, 17, 21, 14, 13, 1, 8, 6, 1, 20, 18, 8, 13, 4, 18, 18, 2, 14, 13, 18, 20, 11, 19, 8, 13, 6, 20, 12, 7, 8, 11, 5, 4, 20, 13, 3, 3, 8, 4, 18, 4, 4, 13, 19, 18, 2, 7, 8, 4, 3, 4, 13, 3, 0, 18, 11, 0, 13, 3, 1, 17, 0, 20, 2, 7, 4, 21, 14, 17, 0, 11, 11, 4, 12, 4, 8, 13, 4, 13, 13, 4, 20, 4, 13, 13, 0, 12, 4, 13, 3, 4, 17, 0, 11, 19, 4, 22, 0, 17, 0, 1, 6, 4, 13, 20, 19, 25, 19, 20, 13, 3, 8, 13, 18, 15, 8, 17, 8, 4, 17, 19, 4, 11, 0, 20, 19, 20, 12, 5, 17, 0, 6, 4, 13, 13, 20, 17, 13, 14, 2, 7, 4, 22, 8, 6, 6, 4, 18, 19, 17, 8, 6, 4, 13, 0, 19, 8, 14, 13, 0, 11, 8, 18, 19, 4, 13, 12, 8, 19, 6, 4, 17, 8, 13, 6, 4, 17, 10, 0, 20, 5, 10, 17, 0, 5, 19

11, 5, 14, 22, 1, 23, 7, 17, 0, 21, 12, 9, 1, 20, 16, 6, 21, 21, 23, 8, 22, 5, 19, 23, 19, 24, 21, 7, 13, 11, 14, 11, 19, 12, 4, 21, 16, 18, 5, 5, 12, 21, 1, 23, 14, 10, 13, 11, 19, 5, 25, 2, 24, 8, 17, 6, 22, 18, 10, 7, 0, 24, 3, 0, 0, 10, 16, 3, 19, 24, 19, 11, 5, 24, 19, 14, 7, 5, 10, 25, 5, 20, 0, 12, 16, 21, 8, 16, 17, 11, 8, 7, 3, 22, 18, 6, 19, 0, 3, 11, 12, 3, 23, 6, 19, 23, 12, 5, 5, 6, 9, 24, 13, 21, 6, 3, 19, 21, 12, 1, 25, 13, 14, 25, 25, 25, 11, 11, 18, 25, 20, 3, 11, 12, 7, 11, 10, 1, 13, 11, 25, 1, 25, 20, 19, 17, 4, 14, 24, 24, 20, 25, 17, 7, 9, 24, 12, 16, 21, 14, 3, 7, 2, 17, 13, 6, 17, 24, 13, 24, 15, 5, 4, 2, 20, 16, 5, 3, 18, 2, 1, 0, 21, 10, 12, 20, 4, 17, 4, 17, 7, 18, 22, 13, 19, 0, 13, 25, 9, 17, 10, 23, 0, 11, 2, 23, 17, 19, 23, 10, 20, 2, 5, 24, 12, 0, 2, 4, 22, 19, 19, 3, 5, 17, 9, 16, 17, 11, 2, 16, 11, 17, 23, 4, 8, 7, 7, 20, 19, 10, 24, 6, 15, 13, 0, 5, 8, 8, 11, 10, 0, 22, 24, 22, 23, 9, 24, 18, 18, 21, 24, 3, 19, 22, 22, 23, 14, 11, 15, 0, 1, 6, 3, 5, 23, 13, 1, 12, 2, 2, 16, 6, 19, 16, 1, 25, 7, 2, 1, 3, 14, 10, 7, 5, 0, 7, 4, 23, 1, 24, 6, 20, 19, 5, 13, 22, 9, 20, 6, 2, 4, 21, 14, 10, 6, 1, 18, 19, 4, 25, 20, 0, 6, 15, 1, 24, 20, 23, 25, 20, 1, 7, 17, 13, 19, 1, 25, 25, 7, 14, 22, 22, 13, 25, 19, 2, 19, 21, 4, 24, 21, 17, 4, 20, 12, 17, 21, 21, 3, 4, 13, 4, 19, 3, 0, 19, 5, 16, 25, 25, 11, 10, 0, 16, 19, 23, 0, 3, 18, 19, 8, 6, 12, 7, 3, 24, 20, 6, 2, 16, 21, 17, 22, 8, 14, 19, 8, 6, 3, 18, 2, 25, 0, 7, 4, 13, 19, 23, 9, 11, 22, 23, 13, 18, 20, 4, 1, 8, 20, 14, 17, 17, 2, 8, 11, 14, 17, 5, 14, 4, 4, 4, 10, 18, 20, 10, 19, 3, 0, 8, 6, 18, 9, 20, 17, 12, 22, 22, 4, 5, 17, 12, 2, 23, 11, 8, 9, 9, 14, 11, 17, 25, 3, 19, 18, 21, 24, 18, 17, 8, 19, 6, 12, 19, 3, 19, 21, 24, 7, 2, 22, 13, 17, 18, 6, 17, 17, 2, 8, 21, 2, 22, 21, 2, 23, 10, 8, 8, 21, 15, 13, 17, 15, 14, 0, 2, 17, 4, 8, 6, 20, 12, 20, 25, 19, 7, 13, 25, 10, 18, 9, 18, 21, 16, 18, 12, 13, 16, 21, 17, 10, 13, 17, 12, 4, 6, 16, 9, 25, 19, 13, 0, 19, 22, 13, 19, 17, 8, 7, 5, 17, 23, 4, 12, 20, 3, 6, 10, 2, 17, 5, 23, 12, 22, 5, 12, 23, 18, 10, 6, 18, 19, 12, 7, 21, 6, 25, 13, 18, 8, 6, 6, 25, 16, 3, 25, 0, 25, 17, 16, 4, 25, 23, 24, 9, 7, 6, 7, 6, 9, 7, 21, 23, 2, 21, 23, 21, 6, 22, 6, 15, 7, 23, 17, 12, 19, 8, 8, 16, 3, 16, 5, 1, 17, 11, 0, 22, 25, 8, 15, 24, 2, 8, 8, 25, 10, 8, 12, 25, 20, 23, 19, 13, 10, 12, 20, 11, 15, 15, 13, 1, 6, 4, 4, 10, 7, 18, 21, 7, 25, 19, 9, 15, 15, 12, 9, 10, 7, 13, 20, 25, 8, 10, 15, 4, 1, 1, 11, 9, 25, 16, 10, 7, 17, 21, 18, 2, 22, 6, 11, 13, 20, 20, 22, 25, 2, 14, 17, 1, 4, 3, 12, 24, 8, 0, 8, 10, 18, 3, 8, 19, 19, 16, 17, 9, 22, 6, 17, 9, 15, 6, 6, 17, 11, 13, 5, 19, 21, 23, 18, 2, 15, 9, 18, 14, 12, 5, 2, 1, 7, 4, 8, 14, 11, 3, 16, 19, 10, 5, 12, 13, 0, 8, 6, 6, 24, 18, 6, 18

Abgabe bis Mittwoch 19.5.2021 bis 14 Uhr per Email an den Tutor, von dem Sie die letzte Korrektur erhielten (nicht unbedingt der, dessen Tutorium Sie besuchen).

Jan Jan-Philipp Brünger
Leonard Simon Ellinghaus
Kallias Stoupas

jbruenger@techfak.de
lellinghaus+krypto@techfak.de
kstoupas+krypto@techfak.de