André Bajorat
Rasmus Diederichsen
Lisa Goerke

Sebastian Höffner
Kristin Schmidt

Lösungen zu Übungsblatt 5
Kryptographische Verfahren

Besprechung 4. Dezember 2015

Aufgabe 5.1. Der Geburtstagsangriff mit konstantem Speicher terminiert

Es sei mit $P(n,k)$ die Wahrscheinlichkeit bezeichnet, bei n Versuchen (n verschiedenen Eingaben) bei einer Hashlänge von 2^k Bits keine Kollision zu erhalten.

$$
\begin{aligned}
P(n,k) &= 1 \cdot \frac{2^k - 1}{2^k} \cdot \ldots \cdot \frac{2^k - n + 1}{2^k} \\
P(n,k) &= \prod_{i=0}^{n-1} \frac{2^k - i}{2^k} \\
&= \prod_{i=1}^{n-1} (1 - \frac{i}{2^k})
\end{aligned}
$$

Da $(1-x)$ durch e^{-x} nach oben abgeschätzt werden kann, gilt

$$
\begin{aligned}
&\leqslant \prod_{i=1}^{n-1} e^{-\frac{i}{2^k}} \\
&= e^{\sum_{i=1}^{n-1} -\frac{i}{2^k}} \\
&= e^{-\frac{1}{2^k} \sum_{i=1}^{n-1} i} \\
&= e^{-\frac{1}{2^k} \frac{n(n-1)}{2}} \\
&\leqslant e^{-\frac{(n-1)^2}{2 \cdot 2^k}}
\end{aligned}
$$

Gesucht ist nun n, sodass $P(n, 128) = \frac{1}{4}$.

$$
\begin{aligned}
e^{-\frac{(n-1)^2}{2 \cdot 2^k}} &= \frac{1}{4} \\
-\frac{(n-1)^2}{2 \cdot 2^k} &= \ln \frac{1}{4} \\
-(n-1)^2 &= 2 \cdot 2^k \cdot \ln \frac{1}{4} \\
-n^2 + 2n - 1 &= 2 \cdot 2^k \cdot \ln \frac{1}{4} \\
n^2 - 2n + 1 &= -2 \cdot 2^k \cdot \ln \frac{1}{4}
\end{aligned}
$$

Mit den üblichen Verfahren, z.B. pq-Formel und Computerunterstützung lässt dies als positive Lösung zu

$$
n_{128} \approx 30.715.843.678.825.642.450 \geqslant 3.0716 \cdot 10^{19}
$$

Man müsste also mehr also über dreißig Trillionen Versuche machen. Analog gelangt man für $k = 160$ zu dem Ergebnis

$$n_{160} \approx 2.012.993.531.335.517.303.552.701 \geqslant 2.013 \cdot 10^{24}$$

oder etwa 2 Quadrillionen Versuche.

Aufgabe 5.2. Der Geburtstagsangriff mit konstantem Speicher findet Kollisionen

Falls es $1 \leqslant 1 < I < J$ mit $x_I = x_J$ und damit $H(x_{I-1}) = H(x_{J-1})$ gibt, so hat die Folge $x_1, \ldots, x_q$ offenbar eine Periode von $J - I$. Der J-te Wert ist also gleich dem I-ten. Falls man die Periodizität schon für $i < I$ annehmen kann, gilt $x_{J-I} = x_{J-I+J-I} = x_{2(J-I)}$.

Allgemein stimmt die Aussage aber nicht. Gilt zum Beispiel $x_7 = x_{12}$, so ist $x_8 = x_{13}, x_9 = x_{14}, \ldots, x_{10} = x_{15}$.