Lösungen, 16.7.2018

108.) Wir ziehen Zufallszahlen x_1, x_2 und erhalten folgende Hashwerte:

x_1	x_2	$h(x_1, x_2)$	
8	22	3	
9	20	16	
1	19	14	
8	12	9	← Kollision
2	7	8	
5	11	9	← Kollision

109.) Angenommen, h_1 ist <u>nicht</u> kollisionsresistent.

Gegeben sei x und $h(x) = z$. Ferner ist $h_1(x) = y$ und $h_2(y) = z$ für ein y.

Da h_1 nicht kollisionsresistent ist, kann man effizient ein $x' \neq x$ finden mit $h_1(x') = h_1(x) = y$. Damit ist $h(x') = z$ und h ist ebenfalls nicht kollisionsresistent. Widerspruch.

110.) $n = 11 \cdot 13 = 143$. Damit ist $\varphi(n) = 10 \cdot 12 = 120 = 2^3 \cdot 3 \cdot 5$. Damit ergibt sich das kleinstmögliche $e > 1$ mit $e \in \mathbb{Z}^*_{\varphi(n)}$ als $e = 7$.

Nun muss $d = e^{-1} \bmod 120$ bestimmt werden:

$120 = 17 \cdot 7 + 1$

Somit $1 = 120 - 17 \cdot 7$ bzw. $e^{-1} \equiv -17 \pmod{120}$

$\equiv 120 - 17 = 103$

Also, $d = \underline{\underline{103}}$.

$m = 9$ unterschreiben: $u = 9^{103} \bmod 143 = \underline{\underline{113}}$

Verblenden: $\tilde{m} = m \cdot z^e \bmod n = 9 \cdot 5^7 \bmod 143 = \underline{137}$

$\tilde{m}$ unterschreiben: $\tilde{u} = \tilde{m}^d \bmod n = 137^{103} \bmod 143 = \underline{136}$

Verblendung entfernen: $\tilde{u} \cdot z^{-1} \bmod n$; hierzu

z^{-1} bestimmen: $143 = 28 \cdot 5 + 3$

$5 = 1 \cdot 3 + 2$

$3 = 1 \cdot 2 + 1$

$\Rightarrow 1 = 3 - 2 = 3 - (5 - 3) = -5 + 2 \cdot 3$

$= -5 + 2 \cdot (143 - 28 \cdot 5) = 2 \cdot 143 - 57 \cdot 5$

Also $z^{-1} \equiv -57 \equiv 143 - 57 = 86$

$\Rightarrow \tilde{u} \cdot z^{-1} \bmod n = 136 \cdot 86 \bmod 143 = \underline{\underline{113}} = u$

111.) Ein Isomorphismus muss Knoten vom Grad d ebenfalls auf einen Knoten vom Grad d abbilden.

Daher besteht nur noch eine Anzahl möglicher Isomorphismen von $(5!)^5 \approx 2^{35}$. Das notwendige Sicherheitsniveau wird nicht erreicht. Man sollte einen <u>regulären</u> Zufallsgraphen erzeugen; also alle Knoten sollten denselben Grad haben, etwa $\log n$ oder $\sqrt{n}$.

112.) Sei $\mathrm{IsoGraph}(G_0) = \mathrm{IsoGraph}(G_1)$ die Menge der zu G_0 bzw. G_1 isomorphen Graphen. Beim echten Protokoll ist H gleichverteilt in $\mathrm{IsoGraph}(G_0)$. Ferner ist b gleichverteilt auf $\{0,1\}$. Die dritte Zufallsvariable τ hängt von H und b ab: es ist τ so, dass $\tau(G_b) = H$. Der Simulator erzeugt ebenfalls b gleichverteilt. Da τ gleichverteilt auf S_n gewählt wird, ist es auch $\tau(G_b) \overset{=H}{}$ auf $\mathrm{IsoGraph}(G_b)$. Ferner hat τ die erwünschte Eigenschaft $\tau(G_0) = H$.