Kryptologie: Übungsblatt 12, Besprechung am 16.7.2018, 10:15, H20

108.) Betrachte die Hashfunktion

$$h(x_1, x_2) = 2^{x_1} \cdot 3^{x_2} \bmod 23$$

mit Definitionsmenge $\mathbb{Z}_{11} \times \mathbb{Z}_{23}$ und Wertemenge $\mathbb{Z}_{23}^*$.
Verwende einen Geburtstagsangriff, um $(x_1, x_2) \neq (y_1, y_2)$ zu finden mit $h(x_1, x_2) = h(y_1, y_2)$.

109.) Sei h eine Hashfunktion, die durch Komposition zweier Hashfunktionen h_1 und h_2 zustande kommt, also erst h_1 anwenden, dann h_2.
Zeigen Sie: wenn h kollisionsresistent ist, dann ist es auch h_1.

110.) In einem RSA-System soll eine blinde Unterschrift realisiert werden. Sei $n = 11 \cdot 13 = 143$ die öffentliche Modulgröße von Teilnehmer B. Bestimme den kleinstmöglichen (öffentlichen) Verschlüsselungsexponenten e sowie den dazu gehörigen (geheimen) Entschlüsselungsexponenten d.
Von B soll das Dokument $m = 9$ unterschrieben werden. Bestimmen Sie die Unterschrift u von B.
Der Teilnehmer A verblendet allerdings zunächst das Dokument m mittels der Zufallszahl $z = 5$ zu $\tilde{m}$. Bestimmen Sie $\tilde{m}$ sowie B's Unterschrift $\tilde{u}$ zu $\tilde{m}$.
Sodann entfernt A wieder die Verblendung und erhält die Unterschrift u zu m. Rechnen Sie nach, dass A tatsächlich u erhält.

111.) Man erzeugt für ein Zero-Knowledge-Protokoll einen Zufallsgraphen G_0 mit 25 Knoten und eine Zufallspermutation $\pi \in S_{25}$. Öffentlich gemacht wird G_0 und $G_1 = \pi(G_0)$. Geheim bleibt π. Da $|S_{25}| = 25! \approx 2^{84}$ vermutet man ein genügend großes Sicherheitsniveau.
Allerdings hat sich der Graph G_0 so ergeben, dass sich dessen Knotenmenge in 5 disjunkte Teilmengen mit jeweils 5 Knoten zerlegen lässt, so dass jede dieser Gruppen einen anderen Knotengrad (=Anzahl Nachbarn des betreffenden Knotens) besitzt. Es kommen also 5 verschiedene Knotengrade d_1, d_2, d_3, d_4, d_5 im Graphen vor. Wie sicher schätzen Sie nun die algorithmische (Un)Möglichkeit ein, einen Isomorphismus zwischen G_0 und G_1 zu finden?
Wie sollte man daher bei der Wahl eines Zufallsgraphen vorgehen?

112.) Beim Zero Knowledge-Protokoll basierend auf Graphisomorphie erzeugt der Simulator-Algorithmus, bei Eingabe von G_0, G_1, ohne Kenntnis des Isomorphismus' zwischen G_0 und G_1, derartige Tripel (H, b, τ) (commitment - challenge - response), die exakt so statistisch verteilt sind wie die Kommunikation, die beim echten Protokoll entsteht (und die die Kenntnis des geheimen Isomorphismus ausnutzt).
Weisen Sie dies nach.