Übungsblatt 6

Kryptographie und Kodierungstheorie
WiSe 16/17

Aufgabe 6.1. Beweisen Sie als Folge des quadratischen Reziprozitätsgesetzes für Primzahlen das verallgemeinerte quadratische Reziprozitätsgesetz

$$\left(\frac{M}{N}\right) = (-1)^{\frac{M-1}{2}\frac{N-1}{2}}\left(\frac{N}{M}\right),$$

wobei M und N positive ungerade Zahlen sind.

Aufgabe 6.2. Beweisen Sie für positive ungerade Zahlen N:

$$\left(\frac{-1}{N}\right) = (-1)^{\frac{N-1}{2}}.$$

Aufgabe 6.3. Verschlüsseln Sie den Bitstring $m = 1010$ mit dem Goldwasser-Micali-Verfahren mit öffentlichem Schlüssel $(n, y) = (10403, 3)$ und zufälligen Zahlen $u_i \in (\mathbb{Z}/n\mathbb{Z})^*$, $i = 1, \ldots, 4$. Entschlüsseln Sie anschließend die Nachricht

$$c = (328, 5057, 1301, 297).$$

Aufgabe 6.4. Für eine Permutation π in S_3 sei e_π die Bitpermutation für Bitstrings der Länge 3. Bestimmen Sie für jedes $\pi \in S_3$ die Anzahl der Kollisionen der Kompressionsfunktion $h_\pi(x) = e_\pi(x) \oplus x$.

Aufgabe 6.5. Betrachten Sie die Hashfunktion

$$h : \{0,1\}^* \to \{0,1\}^*,\ k \mapsto \lfloor 10000(k\frac{1+\sqrt{5}}{2} \bmod 1)\rfloor,$$

wobei die Strings k mit den durch sie dargestellten natürlichen Zahlen identifiziert werden und $r \bmod 1 = r - \lfloor r \rfloor$ ist für eine positive reelle Zahl r. Bestimmen Sie die maximale Länge der Bilder und geben Sie eine Kollision dieser Hashfunktion an.

Aufgabe 6.6. Berechnen Sie die RSA-Signatur (ohne Hashfunktion) von $m = 11111$ mit Modul $n = 28829$ und dem kleinstmöglichen öffentlichen Exponenten e.

Hinweis: Wenn der Schlüsseltext $c \equiv m^e \bmod n$ ist, wie könnte dann das Signaturverfahren mit RSA funktionieren?