



Lösungsskizzen zu Übung 11

Achtung: Die Lösungsskizzen sollen nur die Ideen veranschaulichen und sind daher gelegentlich sehr informell geschrieben; präzisere Lösungen sollten allerdings leicht daraus ableitbar sein.

Aufgabe 1 (Randomisierte RSA-Signaturen)

Ein Angreifer kann hier wie folgt vorgehen. Er wählt eine zufällige Nachricht m^* , so dass das letzte Bit von $H(m^*)$ 1 ist ($H(m^*)$ ist eine ungerade Zahl). Der Angreifer gibt dann m^* und $s^* = H(m^*)^{3^{-1}} \bmod 2^{160}$ als Signatur zurück.

Die Signatur ist korrekt. Zum einen gilt $s^{*3} \bmod 2^{160} = \left(H(m^*)^{3^{-1}}\right)^3 \bmod 2^{160} = H(m^*) \bmod 2^{160}$. Die Rechten 160 Bit der Signatur sind damit schon einmal korrekt. Zum anderen gilt auch $s^* < 2^{160}$ und damit auch $s^{*3} < (2^{160})^3 \leq 2^{480}$. Damit findet bei der Signaturprüfung keine Modulo-Reduktion statt, und es gilt $s^{*3} \bmod N = s^{*3}$.