

10. Übungsblatt zur Vorlesung Kryptologie

Übung 1

Geben Sie ein Beispiel an, dass aus $g \circ f = \text{id}$ nicht unbedingt auch $f \circ g = \text{id}$ folgt.

(Das hat zur Folge, dass nicht automatisch jedes Public-Key-Verfahren auch zur digitalen Signatur genutzt werden kann und umgekehrt.)

Übung 2

Alice hat einen RSA-Schlüssel zu $n = 31 \cdot 41$ und veröffentlicht $e = 17$.

- a1) Ist $s = 751$ eine gültige Signatur zu $m = 111$?
- a2) Ist $s = 615$ eine gültige Signatur zu $m = 321$?
- b) Wie lautet die Signatur s zu $m = 50$?

Übung 3

Alice benutzt das RSA-Signaturverfahren mit der Hashfunktion

$$h : \mathbb{N} \rightarrow \mathbb{Z}_n, h(m) = m^{e_h} \bmod n_h$$

(vgl. Blatt 9, Übung 1), wobei konkret

$$n_h = 223390229630894823575503 \quad \text{und} \quad e_h = 23$$

ist. Als RSA-Schlüssel nutzt sie

$$n_{\text{RSA}} = 922676962174818067510521705931 \quad \text{und} \quad e_{\text{RSA}} = 17.$$

Alice signiert die Nachricht $m = 10^{50}$ und erhält als Signatur

$$s = 122213354635279262673569254549.$$

- a) Verifizieren Sie, dass s tatsächlich die Signatur zu m ist.
- b) Finden Sie eine andere Nachricht m' , die die gleiche Signatur s besitzt?

Übung 4

Zum Fälschen einer digitalen RSA-Signatur mit Hashfunktion h , kann folgender *meet-in-the-middle-Angriff* ausgeführt werden:

Wähle zufällig Werte s_i und berechne $h_i = s_i^e \bmod n$.

Wähle Nachrichten m_j und berechne $h(m_j)$.

Suche i_0 und j_0 mit $h_{i_0} = h(m_{j_0})$.

Dann ist s_{i_0} eine gültige Signatur von m_{j_0} .

Schätzen Sie die Größenordnung des Aufwands für einen erfolgreichen Angriff in Abhängigkeit von n ab. Ist $n \approx 2^{100}$ groß genug, um den Angriff praktisch unmöglich zu machen?