FH AACHEN
UNIVERSITY OF APPLIED SCIENCES

Fachbereich Elektrotechnik
und Informationstechnik

Prof. Georg Hoever

WS 2023/24
13.12.2023

10. Übungsblatt zur Vorlesung Kryptologie

Übung 1

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

(Das hat zur Folge, dass nicht automatisch jedes Public-Key-Verfahren auch zur digialen 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

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

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

$$n_h = 22339022963089482357 5503 \qquad \text{und} \qquad e_h = 23$$

ist. Als RSA-Schlüssel nutzt sie

$$n_{\mathrm{RSA}} \ = \ 92267696217481806751052170 5931 \qquad \text{und} \qquad e_{\mathrm{RSA}} \ = \ 17.$$

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

$$s \ = \ 12221335463527926267356925 4549.$$

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?