FH AACHEN
UNIVERSITY OF APPLIED SCIENCES

Fachbereich Elektrotechnik
und Informationstechnik

Prof. Georg Hoever

WS 2023/24
13.12.2023

Musterlösung zum 10. Übungsblatt zur Vorlesung Kryptologie

Übung 1

Sei

$$f : \mathbb{Z} \to \mathbb{Z},\ f(x) = 2 \cdot x, \qquad \text{und} \qquad g : \mathbb{Z} \to \mathbb{Z},\ g(x) = \lfloor \tfrac{1}{2} \cdot x \rfloor,$$

wobei $\lfloor a \rfloor$ Abrunden von a bedeutet, falls a keine ganze Zahl ist.

Dann ist

$$g \circ f(x) = g(2 \cdot x) = \lfloor \tfrac{1}{2} \cdot 2 \cdot x \rfloor = \lfloor x \rfloor = x,$$

also $g \circ f = \mathrm{id}$, aber z.B.

$$f \circ g(3) = g(\lfloor \tfrac{1}{2} \cdot 3 \rfloor) = g(\lfloor 1.5 \rfloor) = g(1) = 2 \cdot 1 = 2 \neq 3,$$

also $f \circ g \neq \mathrm{id}$.

Übung 2

a1) Wegen $751^{17} \bmod n = 111$ ist $s = 751$ gültige Signatur zu $m = 111$.

a2) Wegen $615^{17} \bmod n = 533 \neq 321$ ist $s = 615$ keine gültige Signatur zu $m = 321$.

b) Um die Signatur zu berechnen, braucht man den privaten Schlüssel von Alice:

Es ist $f = 30 \cdot 40 = 1200$. Die Gleichung $d \cdot 17 = 1 \bmod 1200$ hat die Lösung $d = 353$, d.h. Alice privater Schlüssel ist $d = 353$.

Damit kann man die Signatur berechnen durch

$$s = 50^d \bmod n = 50^{353} \bmod 1271 = 9.$$

Tatsächlich ist dann $9^{17} \bmod 1271 = 50 = m$.

Übung 3

a) Es ist zu überprüfen, ob

$$h(m) = m^{e_h} \bmod n_h \stackrel{?}{=} s^{e_{\mathrm{RSA}}} \bmod n_{\mathrm{RSA}}$$

ist. Tatsächlich erhält man

$$(10^{50})^{23} \bmod n_h = 184479150937238321619147 = s^{17} \bmod n_{\mathrm{RSA}}.$$

b) Wie schon bei Blatt 9, Übung 1, erwähnt, hat $m' = m + n_h$ den gleichen Hashwert wie m, denn

$$h(m') \;=\; h(m + n_h) \;=\; (m + n_h)^{e_h} \bmod n_h \;=\; m^{e_h} \bmod n_h \;=\; h(m).$$

Konkret hat hier

$$m' \;=\; m + n_h \;=\; 1000000000000000000000000000022339022963089482357550 3$$

die gleiche Signatur wie m.

Übung 4

Wie bei der Geburtstagsattacke erhält man unter den Werten der s_i und h_j eine Kollision mit Wahrscheinlichkeit größer 0.5, wenn man ca. $1.2 \cdot \sqrt{n}$ Werte berechnet hat. In der Hälfte der Fälle ist das eine gewünschte Kollision von einem s_{i_0} zu einem h_{j_0}.

Bei $n \approx 2^{100}$ braucht man also ca. $\sqrt{n} \approx 2^{50}$ Berechnungen, was praktisch möglich ist. n ist also zu klein.