

Aufgabe 15: (8 Punkte)

- (a) Gegeben seien die beiden Kommunikationspartner Alice und Bob mit ihren RSA-Schlüsselpaaren (K_E^A, K_D^A) bzw. (K_E^B, K_D^B) , wobei n der RSA-Modul von Bob sei. Die beiden setzen RSA zum Verschlüsseln und Signieren ein.

Betrachten Sie folgenden Angriff von Eve, die die Verschlüsselung C einer Nachricht P von Alice an Bob abfängt.

1. Alice sendet an Bob den Geheimtext $C := RSA(P, K_E^B)$.
2. Eve fängt die Nachricht C ab und berechnet für eine zufällige Zahl $r < n$ mit $\text{ggT}(r, n) = 1$ die Werte $s := RSA(r, K_E^B)$ und $\tilde{C} := (sC) \bmod n$.
3. Eve bringt Bob dazu, die Nachricht \tilde{C} zu signieren und ihr die Signatur $sig := RSA(\tilde{C}, K_D^B)$ zurückzuschicken.

Wie kann Eve aus der Signatur sig den Klartext P entschlüsseln? Geben Sie zwei Möglichkeiten an, wie Alice und Bob diesen Angriff verhindern können.

- (b) Gegeben sei eine natürliche Zahl n und eine Nachricht $M = (M_1, \dots, M_m)$ bestehend aus natürlichen Zahlen $M_i < n$ für $i = 1, \dots, m$. Der Hashwert $h(M)$ sei definiert als h_m wobei

$$h_1 := M_1, \quad h_i := (h_{i-1}^2 \bmod n) \oplus M_i \quad \text{für } i = 2, \dots, m.$$

Zeigen oder widerlegen Sie: Die Hashfunktion h ist stark kollisionsresistent.

Aufgabe 16: (12 Punkte)

Betrachten Sie die diskrete Quadratfunktion $f(x) = x^2 \bmod n$, wobei $n = pq$ das Produkt von zwei Primzahlen $p \neq q$ mit $p, q > 2$ ist.

- (a) Zeichnen Sie den Funktionsgraphen von f für $p = 5, q = 7$.
- (b) Wie viele Quadratwurzeln modulo n kann eine Zahl y besitzen (d.h. wie viele Lösungen $x \in \mathbb{Z}_n$ kann eine Kongruenz der Form $y = x^2 \bmod n$ haben)? Diskutieren Sie alle Fälle, die für eine gegebene Zahl y auftreten können.
- (c) Zeigen Sie, dass sich mit Hilfe der Faktorisierung von n leicht alle Quadratwurzeln einer gegebenen Zahl y berechnen lassen. Dabei soll die Tatsache benutzt werden, dass sich in Restklassenkörpern leicht Quadratwurzeln berechnen lassen. (Hinweis: Chinesischer Restsatz)
- (d) Zeigen Sie umgekehrt, dass sich mit Hilfe eines Verfahrens zur Bestimmung einer Quadratwurzel eine Zahl n leicht faktorisieren lässt.
- (e) Wenden Sie Fall (c) auf folgendes Beispiel an: Berechnen Sie mit Hilfe der Faktorisierung von $n = 77$ in \mathbb{Z}_{77} alle Quadratwurzeln der Zahl $y = 60$, d.h. alle Lösungen $x \in \mathbb{Z}_n$ der Kongruenz $x^2 \bmod n = 60$.