Kryptographie **Blatt 3B**

hhu Düsseldorf
WiSe 2023/24

Abgabe: bis Montag 06.11.2023, vor der Vorlesung

Vorlesungswebseite: `http://reh.math.uni-duesseldorf.de/~khalupczok/krypto/`

Aufgabe 3: Das Fiat–Shamir-Verfahren

Sei n eine natürliche Zahl, die Alice und Bob beide kennen. Bekannt ist, dass n Produkt zweier großer Primzahlen $p \neq q$ ist, die Faktoren sind aber unbekannt und so groß, dass niemand n in angemessener Zeit faktorisieren kann.
Alice wählt für sich das Geheimnis s aus $\mathbb{Z}_n^\times$.
Sie möchte Bob davon überzeugen, dass sie das Geheimnis s kennt, ohne es preiszugeben. Dazu berechnet Alice $v \equiv s^2 \bmod n$. Sie behält s geheim und gibt v öffentlich bekannt, insbesondere Bob kennt v. Die Daten n, v könnten öffentlich zugängliche Systemkonstanten sein.

Eine Runde des Verfahrens:

> Alice wählt eine Zufallszahl r aus $\mathbb{Z}_n^\times$, behält diese für sich und schickt das Quadrat $x \equiv r^2 \bmod n$ an Bob. Bob wählt zufällig ein Bit $b \in \{0, 1\}$, etwa per Münzwurf, und sendet es an Alice. Falls $b = 0$ ist, sendet Alice den Wert $y := r$ an Bob, andernfalls den Wert $y :\equiv rs \bmod n$.
> Bob verifiziert die Antwort: Er überprüft die Richtigkeit von $y^2 \equiv xv^b \bmod n$. Stimmt dies nicht, würde Bob nicht anerkennen, dass Alice das Geheimnis s kennt.

Weil Alice das Geheimnis s kennt, kann sie in beiden Fällen korrekt antworten, da $y^2 \equiv (rs^b)^2 \equiv r^2 s^{2b} \equiv r^2 v^b \equiv xv^b \bmod n$ gilt.

• Zeigen Sie, dass sich eine Betrügerin Eva, die sich als Alice ausgibt, auf genau eine der beiden Fragen $b = 0$ oder $b = 1$ von Bob korrekt antworten kann, durch Begründung folgender Behauptungen.

(a) Falls Eva beide Fragen korrekt mit y_0 bzw. y_1 beantworten könnte, wüsste sie bereits eine Wurzel von v mod n.

(b) Wenn Eva vermutet, dass Bob das Bit b schicken wird, präpariert sie entsprechend ihre Antwort: Sie schickt $x \equiv r^2 v^{-b} \bmod n$ an Bob und dann $y = r$. Damit wird Bob keinen Verdacht schöpfen, wenn Bob b schickt, andernfalls klappt die Verifikation nicht.

Wegen (a) kann Eva nur mit Wahrscheinlichkeit $\leq 1/2$ betrügen, wegen (b) auch mindestens mit Wahrscheinlichkeit $1/2$. In t vielen Runden beträgt die Wahrscheinlichkeit, dass Eva betrügen kann, also nur $1/2^t$.

• Beantworten und begründen Sie:

(c) Wüsste Eva die Primfaktoren der Zahl n, könnte sie in jeder Runde richtig antworten und so betrügen?

(d) Wer von Alice und Bob darf die Primfaktoren von n kennen?

• Spielen Sie ein Beispiel einer Runde des Verfahrens mit konkreten Zahlen p, q, s einmal rechnerisch durch.