Prof. Dr. Rüdiger Weis

Sicherheit in Verteilten Systemen

Sommersemester 2012

Übungsblatt 4

Advanced Public Key Cryptography

Aufgabe 1 (42 Punkte) Elektronischer Münzwurf

Ein Disput zwischen Alice und Bob soll durch einen elektronischen Münzwurf entschieden werden.

1. Alice wählt Primzahlen p und q.

   Alice $\rightarrow$ Bob: $n = pq$.

   (Intention: Bob gewinnt $\Leftrightarrow$ Bob findet Teiler $t|n$, $1 < t < n$.)

2. Bob wählt zufällig $x \in Z_n$.

   Ist $\text{ggT}(x, n) > 1$ hat Bob bereits gewonnen.
   Sonst: Bob $\rightarrow$ Alice: $y = x^2 \bmod n$.

3. Alice berechnet $r_1, \ldots, r_4$ mit ${r_i}^2 \equiv y \bmod n$.

   Alice $\rightarrow$ Bob: $r \in \{r_i\}$ (zufällig gewählt).

4. Bob überprüft $r^2 \equiv y \bmod n$.

5. Ist $r \not\equiv \pm x \bmod n$, gewinnt Bob: $\text{ggT}(r + x, n) \in \{p, q\}$.

6. Kann Bob keinen Faktor p bzw. q angeben, muss Alice dies tun.
   Sie gewinnt nur, wenn $n = pq$ gilt und p und q teilerfremd sind.
   Andernfalls verliert sie.

Schreiben Sie ein entsprechendes Python-Programm und testen Sie es, indem Sie verschiedene Implementierungen gegeneinander antreten lassen.

Abgabe

per mail mit Subjekt "S12B04" an rweis@beuth-hochschule.de
bitte bis: **Mi 29. Juni 2012, 22:22.**