Wolfgang K. Seiler
Tel. 2515

A5, C201

17. Mai 2013

12. Übungsblatt Kryptologie

Aufgabe 1: *(8 Punkte)*

a) $f: \mathbb{F}_2^m \to \mathbb{F}_2^n$ sei eine Funktion und $m >> n$. Welche Bedingungen muß f erfüllen, damit man diese Funktion als ein kryptographisch sicheres Hashverfahren bezeichnen kann?

b) Erläutern Sie, wie man mit Hilfe von Rijndael ein kryptographisch sicheres Hashverfahren konstruieren kann!

Aufgabe 2: *(5 Punkte)*

Beim Münzwurf per Telephon wählt A zufällig die beiden Primzahlen $p = 44483$ und $q = 77783$, schickt deren Produkt $N = 3460021189$ an B, und erhält von diesem die Zahl $y = 1831904234$, die B als Quadrat modulo N von $x = 12345678$ konstruiert hat. Welche Zahlen kann A nun an B schicken, und bei welchen Wahlen hat er gewonnen?

Aufgabe 3: *(4 Punkte)*

Für das in der Vorlesung behandelte Zero Knowledge Protokoll kennen Sie den öffentlichen Schlüssel $y = x^2 \bmod N$ einer Person, $y = 110592674$ und $N = 670726081$. Sie wollen sich als diese Person ausgeben, und Sie wissen, daß der Verifizierer, wenn Sie ihm eine Zahl $v = u^2 \bmod N$ senden, immer nach einer Wurzel aus vy frägt. Konstruieren Sie eine Zahl v, für die Sie diese Frage ohne Kenntnis von x beantworten können!

Aufgabe 4: *(3 Punkte)*

Ein quantenmechanisches System sei beschrieben durch einen Hermiteschen Vektorraum V; das Hermitesche Produkt zweier Vektoren $|v\rangle$ und $|w\rangle$ aus V sei $\langle v \mid w\rangle$. Eine physikalische Größe f werde beschrieben durch die unitäre Matrix A mit Eigenwerten λ_i; die zugehörigen Eigenvektoren seien $|w_i\rangle$, wobei $\langle w_i \mid w_i\rangle = 1$ sei. Befindet sich das System in einem Zustand $|v\rangle$, von dem wir der Einfachheit halber ebenfalls annehmen wollen, daß $\langle v \mid v\rangle = 1$ ist, erhalten wir bei der Messung von f einen der Werte λ_i, wobei die Wahrscheinlichkeit eines speziellen Eigenwerts λ_i gleich der Summe p_i aller jener Zahlen $\langle v \mid w_j\rangle \cdot \overline{\langle v \mid w_j\rangle}$ ist, für die $|w_j\rangle$ ein Eigenvektor zum Eigenwert λ_i ist. Zeigen Sie, daß die p_i in der Tat Wahrscheinlichkeiten sind, d.h. alle p_i sind nichtnegativ, und ihre Summe ist eins.

Abgabe bis zum Freitag, dem 24. Mai 2013, um 11.55 Uhr