Wolfgang K. Seiler
Tel. 2515

A5, C201

2. Dezember 2010

12. Übungsblatt Kryptologie

Aufgabe 1: *(3 Punkte)*

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

Aufgabe 2: *(4 Punkte)*

Bei der Quantenkryptographie werden einzelne Photonen durch kurze Laserblitze simuliert. Damit ist die Anzahl der Photonen pro Blitz nicht konstant gleich eins, sondern ist durch eine Poisson-Verteilung gegeben. Beim BB84-Protokoll wählt man meist eine mit Parameter $\lambda = 1/10$.

a) Wie viele von Tausend Lichtblitzen enthalten mindestens ein Photon?

b) Wie viele von Tausend Lichtblitzen enthalten genau ein Photon?

c) Beim SARG04-Protokoll arbeitet man oft mit $\lambda = 1/5$. Hier kann ein Gegner allerdings den Zustand eines Photons nur dann unbemerkt messen, wenn der Blitz mindestens drei Photonen enthält. Wie viele von Tausend Blitzen enthalten mindestens ein Photon, und wie viele davon enthalten weniger als drei?

Aufgabe 3: *(6 Punkte)*

a) Zeigen Sie durch vollständige Induktion nach der Dimension, daß zwei diagonalisierbare Matrizen genau dann miteinander vertauschbar sind, wenn es eine Basis gibt, deren Elemente Eigenvektoren beider Matrizen sind.

b) Zwei Meßgrößen eines quantenmechanischen Systems seien beschrieben durch die beiden Hermiteschen und damit diagonalisierbaren Matrizen A und B. Zeigen Sie, daß die Wahrscheinlichkeit eines Paars (a, b) von Meßergebnissen für beide Größen genau dann nicht von der Reihenfolge der Messungen abhängt, wenn $AB = BA$ ist!

Aufgabe 4: *(3 Punkte)*

a) Eine Basis eines Hermiteschen Vektorraums heißt *Orthogonalbasis,* wenn für zwei verschiedene Basisvektoren $|b_1\rangle$ und $|b_2\rangle$ stets $\langle b_1|b_2\rangle = 0$ ist. Finden Sie eine Orthogonalbasis von $\mathbb{C}^2$, die den Vektor $\binom{1}{i}$ enthält!

b) Zeigen Sie: Für jeden Vektor v aus einem Hermiteschen Vektorraum V ist die Menge $v^\perp = \{u \in V \mid \langle u|v\rangle = 0\}$ ein Untervektorraum.

Aufgabe 5: *(4 Punkte)*

a) Berechnen Sie, soweit möglich, die Ordnungen der Zahlen 2 bis 7 modulo 15, und versuchen Sie, damit die Zahl 15 nach dem Algorithmus von Shor zu faktorisieren!

b) Erklären Sie, warum in einigen Fällen *a priori* klar war, daß Sie keinen Erfolg haben!

Abgabe bis zum Donnerstag, dem 9. Dezember 2010, um 15.30 Uhr