Spezielle Aspekte: Kryptographie *SoSe 2011*
PD Dr. Barbara Baumeister
Tutoren: Patrick Wegener, Philipp Neumann, Patrick Odenbach

11. Übungsblatt

Abgabe: Mittwoch, 22.6.11

Aufgabe 1 *Wählt man aus einer m-elementigen Menge M mit Zurücklegen $k \leq m$ Elemente, so ist die Wahrscheinlichkeit $p_{m,k}$ dafür, dass die Elemente alle voneinander verschieden sind, gleich*

$$p_{m,k} = \prod_{i=0}^{k-1}(1 - \frac{i}{m}).$$

Falls k viel kleiner ist als m, dann gilt

$$p_{m,k} \approx exp(-\frac{k(k-1)}{2m}).$$

(a) Zeigen Sie, falls $p_{m,k} = 1/2$, dann ist $k \approx \frac{6}{5}\sqrt{m}$.

(b) Wie viele Personen sollten sich in einem Raum aufhalten, damit die Wahrscheinlichkeit, dass zwei am selben Tag Geburtstag haben, etwa 1/2 ist?

Das sogenannte Geburtstagsparadoxon kann genutzt werden, um eine Kollision einer Hashfunktion zu finden - siehe die Präsenzübung.

Aufgabe 2 *Sei S_3 die Menge der Bijektionen von der Menge $\{1, 2, 3\}$ in sich; also die Menge der Abbildungen von einem Dreieck in sich selber, wobei die Ecken mit $1, 2, 3$ durchnummeriert sind. Jede solche Bijektion heißt Permutation.*

Für eine Permutation π in S_3 sei e_π die Bitpermutation für Bitstrings der Länge 3, d.h. $e_\pi(x_1, x_2, x_3) = (x_{\pi(1)}, x_{\pi(2)}, x_{\pi(3)})$. Für jedes $x \in \mathbb{Z}_2^3$ und $\pi \in S_3$ setzte $h_\pi(x) = e_\pi(x) + x \subseteq \mathbb{Z}_2^3$.

Bestimmen Sie für jedes $\pi \in S_3$ die Anzahl der Kollisionen von $h_\pi(x)$, d.h. die Anzahl der Paare (x, y) mit

$$h_\pi(x) = h_\pi(y).$$

Aufgabe 3 *Alice besitze den öffentlichen Schlüssel* $(p, \alpha, \beta) = (107, 2, 80)$. *Alice signiert die Nachricht* x *mit* $(9, 93)$. *Welche der folgenden Nachrichten* $x = 10$, $x = 83$, $x = 17$ *ist sicher nicht von Alice, also gefälscht?*

Aufgabe 4 *Angenommen, Alice benutzt das gleiche* k *bei der ElGamal-Signatur zweier verschiedener Nachrichten* x *und* y. *Unter welchen Voraussetzungen an* x *und* y *kann Oskar die Zufallszahl* k *finden?*