Prof. Dr. Johannes Blömer
Nils Löken, Peter Günther

April 10th, 2016
submission due: April 19th, 2016: 11 a.m.

Cryptography - Provable Security

SS 2016

Handout 1

Exercise 1:
Let E and A be two events and $\overline{A}$ denote the event that A does not occur. Prove the following (in-)equalities:

a) $\Pr[E] = \Pr[E \mid A] \cdot \Pr[A] + \Pr\left[E \mid \overline{A}\right] \cdot \Pr\left[\overline{A}\right]$

b) $\Pr[E] = \Pr\left[E \mid \overline{A}\right] + \left(\Pr[E \mid A] - \Pr\left[E \mid \overline{A}\right]\right) \cdot \Pr[A]$

c) $\Pr[E] \leq \Pr[E \mid A] + \Pr\left[\overline{A}\right]$

Exercise 2:
Consider the following experiment: Given a bin containing black and white balls. Draw a ball from the bin, check the color and put the ball back. Repeat until a black ball is drawn.

a) If a black ball is drawn with probability p, how many repetitions are required, on expectation, until the experiment stops?

b) We now want to perform only a finite number of repetitions. Show that after $1/p$ repetitions with probability at least $1 - 1/e$ at least one repetition yielded a black ball.

Exercise 3:
Let $A_1, \ldots, A_n$ be arbitrary events.

a) Show that $\Pr\{A_1 \cup A_2 \cup \cdots \cup A_n\} \leq \sum_{i=1}^{n} \Pr\{A_i\}$.

b) Show that $\Pr\{A_1 \cap A_2 \cap \cdots \cap A_n\} = \Pr\{A_1\} \prod_{i=2}^{n} \Pr\{A_i | \bigcap_{j=1}^{i-1} A_j\}$.

Exercise 4:

a) Show that $1 - x \leq e^{-x}$

b) Show that for $0 \leq x \leq 1$ it holds that $e^{-x} \leq 1 - x/2$.

Exercise 5:
Let S be a finite set of size n and draw $q \leq \sqrt{2n}$ elements $x_1, \ldots, x_q$ uniformly at random from S. Let $X = \{x_1, \ldots, x_q\}$. Let E be the event of a *collision*, i.e., the event that $|X| < q$. Show that

$$\frac{q(q-1)}{4n} \leq \Pr\{E\} \leq \frac{q^2}{2n}.$$

by proving the following lemmas:

a) For fixed $i < j \leq q$ it holds that $\Pr\{x_i = x_j\} = \frac{1}{n}$.

b) $\Pr\{E\} \leq \binom{q}{2}\frac{1}{n} \leq \frac{q^2}{2n}$ (Hint: use Exercise 3.a)

c) For $1 \leq i \leq q$ let A_i be the event that no collision occurs in the first i elements, i.e., $|\{x_1, \ldots, x_i\}| = i$. It holds that $\Pr\{A_{i+1}|A_i\} = 1 - \frac{i}{n}$ and

$$\Pr\{A_q\} = \prod_{i=1}^{q-1}\left(1 - \frac{i}{n}\right) \leq \prod_{i=1}^{q-1} e^{-i/n} = e^{-q(q-1)/(2n)}$$

Hint: For the first equality, use Exercise 3.b. For the inequality, use Exercise 4. For the last equality, use Gauss.

d) $1 - \Pr\{A_q\} \geq \frac{q(q-1)}{4n}$ (Hint: use Exercise 4)