Problem Set 4

We will work on the following exercises together during the work sessions on Tuesday.

The last questions are marked as homework exercises. Your homework must be handed in within one week **electronically via Canvas before Thursday, 14 September 2017, 20:00h**. This deadline is strict and late submissions are graded with a 0. At the end of the course, the lowest of all the homework grades will be dropped.

You are strongly encouraged to work together on the exercises, including the homework. However, after this discussion phase, you have to write down and submit your own individual solution.

Problem 1: Exercise 3.9 from [KL]

Prove *unconditionally* the existence of a pseudorandom function $F : \{0,1\}^* \times \{0,1\} \to \{0,1\}$ with $\ell_{key}(n) = n$ and $\ell_{in}(n) = O(\log n)$. **Hint:** Implement a uniform function with logarithmic input length.

Problem 2: Exercise 3.14 from [KL]

Prove that if F is a length-preserving pseudorandom function, then $G(s) \stackrel{\text{def}}{=} F_s(1)\|F_s(2)\|\cdots\|F_s(\ell)$ is a pseudorandom generator with expansion factor $\ell \cdot n$.

Problem 3: Exercise 3.16 from [KL]

Prove Proposition 3.27: *If F is a pseudorandom permutation and additionally $\ell_{in}(n) \geq n$, then F is also a pseudorandom function.*

Hint: Use the results of Appendix A.4.