Heads and tails, summer 2015

PROF. DR. JOACHIM VON ZUR GATHEN AND DR. DANIEL LOEBENBERGER

12. Exercise sheet
Hand in solutions until Sunday, 13 July 2015, 23:59:59

Exercise 12.1 (Going to Munich). (20 points)

Drive to Munich and give the talk you prepared in Exercise 11.1 at Crypto-Day 2015. Have fun there. Report on the event in the upcoming tutorial. 20

Alternatively, you might want to work on the following exercise.

Exercise 12.2 (Some questions on pseudorandom generators). (20 points)

(i) What is a pseudorandom generator? 20

(ii) State at least two candidates for pseudorandom generators.

(iii) State criteria for a cryptographically good pseudorandom generator? Why can it happen, that a generator is perfect for simulation, but should not be used in cryptography?

(iv) What is an ε-distinguisher for two distributions X and Y over $\{0,1\}^n$? What is a δ-predictor for the distribution X?

(v) Given a δ-predictor for the ith bit of a distribution X, how can you get a ε-distinguisher between this distribution and the uniform distribution? Give an ε for the predictor.

(vi) Is it possible to derive a δ-predictor for one of the bits from a given ε-distinguisher between X and the uniform distribution? How?

(vii) What is a (k, n, s, t)-design D? Does a sufficiently large amount of designs with small values for k and large values for n exist?

(viii) What is the hardness of a function $f\colon \{0,1\}^s \to \{0,1\}$?

(ix) Given a design D and a (hard) function $f\colon \{0,1\}^s \to \{0,1\}$, how can you design a generator $\{0,1\}^k \to \{0,1\}^n$?

(x) What does the theorem of Nisan and Wigderson say?

(xi) Invent on your own a number of suitable questions on pseudorandom generators.