Heads and tails, summer 2015

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

11. Exercise sheet
Hand in solutions until Sunday, 06 July 2015, 23:59:59

Exercise 11.1 (Creating a twenty minute talk). (20 points)

For Crypto-Day in Munich, we need to create a twenty minute talk with our findings. Use the latex beamer template available at 20

`https://cosec.bit.uni-bonn.de/?id=1016`

Hint: This might be only interesting for those who travel to Munich. However, it is also a good exercise to create a talk on your own.

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

Exercise 11.2 (Horoscopes). (20 points)

You are to investigate if horoscopes really predict the future or if they act more like pseudorandom generators. There is nothing like "the one correct answer" for this task. Experiment on this question. 20

Thus the generator is a horoscope H and the distinguisher L is life. Take a horoscope of last week (or last month or last year) and ask you friends to what extent the horoscope was true for them.

Several approaches to this task are possible. Here is just one suggestion.

Every horoscope consists of twelve parts $H_1, \ldots, H_{12}$, one for each zodiac sign S_i. For each S_i, prepare a sheet B_i that consists of H_i and a randomly chosen $H_i' \xleftarrow{\$} \{H_1, \ldots, H_{12}\}$. (Then $H_i = H_i'$ with probability $\frac{1}{12}$.) You roll a die to determine which one is the first on the sheet. Then you show the sheet B_i to as many of your friends as possible whose zodiac sign is S_i. Ask the friend to tell you to which extent (in percent) the two statements were true for them. In the end you compute the value of the distinguisher on both distributions H and H'. (The distinguisher's results will be numbers between 0 and 100.)

What do you observe? Which further analysis could be interesting? Why? To which degree do your results fit with the concept of pseudorandom generators? Do you get a predictor?