Heads and Tails, summer 2009

PROF. DR. JOACHIM VON ZUR GATHEN, DANIEL LOEBENBERGER

12. Exercise sheet
Hand in solutions until Sunday, 19 July 2009, 24:00h.

Exercise 12.1 (Hash crisis). (10 points)

In the lecture we have touched cryptographic hash functions.

(i) Lookup the definitions for MD5, SHA-1 and SHA-2. Describe which properties we would like to have for a hash function. Which of the three functions would you still use nowadays? $\boxed{5}$

(ii) Read the article Arjen Lenstra, Xiaoyun Wand & Benne de Weger, *Colliding X.509 Certificates* <`http://eprint.iacr.org/2005/067.pdf`> and give a short survey. $\boxed{5}$

Exercise 12.2 (Questions on pseudorandom generators). (0+19 points)

(i) What is a pseudorandom generator? $\boxed{+1}$

(ii) State at least two candidates for pseudorandom generators. $\boxed{+2}$

(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? $\boxed{+1}$

(iv) What is a ε-distinguisher for two distributions X and Y over $\{0,1\}^n$? $\boxed{+1}$

(v) What is a δ-predictor for the distribution X? $\boxed{+1}$

(vi) 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. $\boxed{+2}$

(vii) 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? $\boxed{+2}$

(viii) What is a (k, n, s, t)-design D? $\boxed{+1}$

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

(x) Given a design D and a (hard) function $f\colon \{0,1\}^s \to \{0,1\}$, how can you design a generator $\{0,1\}^k \to \{0,1\}^n$? $\boxed{+2}$

(xi) Does a sufficiently large amount of designs with small values for k and large values for n exist? $\boxed{+1}$

(xii) What does the theorem of Nisan and Wigderson say? $\boxed{+1}$

(xiii) What is the purpose of an extractor? $\boxed{+1}$

(xiv) Describe one construction for a good extractor. $\boxed{+2}$