Leipzig University
Institute of Computer Science
Winter Term 2020/21

Prof. Dr. Andreas Maletti
Fabian Tronicke

Cryptography

Exercise Sheet 3

will be discussed on November 17, 2020

Exercise 3.1

Is one-time pad still perfectly secret if multiple messages are encrypted with the same key? What do you think? What are possible (if there are any) attacks?

Exercise 3.2

Which of these functions are negligible?

(a) 2^{-n}

(b) $2^{-\sqrt{n}}$

(c) $n^{-\log n}$

(d) $\log n^{-\log n}$

(e) n^{-2}

(f) 1.01^{-n}

Exercise 3.3

Let $f : \mathbb{N} \to \mathbb{R}_{\geq 0}$. Proof that these statements are equivalent:

(i) f is negligible.

(ii) For all $c \in \mathbb{N}$ there exists $n_0 \in \mathbb{N}$ such that $f(n) < n^{-c}$ for all $n \in \mathbb{N}$ with $n \geq n_0$.

(iii) For all $c \in \mathbb{N}$ we have $\lim_{n \to \infty} f(n)n^c = 0$.

Exercise 3.4

Let $f, g : \mathbb{N} \to \mathbb{R}_{\geq 0}$ be two negligible functions, $h : \mathbb{N} \to \mathbb{R}$ any function and $r : \mathbb{N} \to \mathbb{R}_{\geq 0}$ a positive polynomial. Proof or refute:

(i) Is $f + g$ negligible?

(ii) Is $f \cdot g$ negligible?

(iii) Is $f + h$ negligible?

(iv) Is $f \cdot h$ negligible?

(v) Is $f + r$ negligible?

(vi) Is $f \cdot r$ negligible?