Leipzig University
Institute of Computer Science
Winter Term 2020/21

Prof. Dr. Andreas Maletti
Fabian Tronicke

Cryptography

Exercise Sheet 8

will be discussed on January 12, 2021

Exercise 8.1

(a) Prove Theorem §8.3 (Unconditionally secure one-time MAC).

(b) How could an adversary break the system with two queries to the mac-oracle?

(c) Modify construction §8.2 (One-time MAC) such that it is secure against any adversary that may query the mac-oracle *at most twice*.
Hint: Interpret the mac-function as a line and generalize this idea.

(d) Why did we define the mac-function modulo q_n (q_n prime)? Why not modulo any non-prime? Why not without the modulo operation?

Exercise 8.2

Prove that the encrypt-then-authenticate-scheme is unforgeable if provided with any encryption scheme (even if not CPA-secure) and any secure MAC.