Leipzig University
Institute of Computer Science
Winter Term 2020/21

Prof. Dr. Andreas Maletti
Fabian Tronicke

Cryptography

Exercise Sheet 9

will be discussed on January 19, 2021

Exercise 9.1

Let h, h' be two collision-resistant hash functions.

(a) Is $\hat{h}$ defined by $\hat{h}_n(m) := h_n(h'_n(m))$ collision resistant?

(b) Is $\hat{\hat{h}}$ defined by $\hat{\hat{h}}_n(m) := h_n(m)h'_n(m)$ collision resistant?

Exercise 9.2

Prove the following formula for Euler's totient function:
Let $n = \prod_{i=1}^{k} p_i^{e_i}$ with p_i prime and $e_i \geq 1$ be the prime factorization of $n \in \mathbb{N}$. Then

$$\phi(n) = \prod_{i=1}^{k} p_i^{e_i - 1}(p_i - 1). \tag{1}$$

A good start is to show that for a prime p and integer $e \geq 1$

$$\phi(p^e) = p^{e-1}(p - 1). \tag{2}$$

Now try to prove that for p, q coprime ($\gcd(p, q) = 1$)

$$\phi(pq) = \phi(p) \cdot \phi(q) \tag{3}$$

holds.
With (2) and (3) you can now prove (1).

Exercise 9.3

Prove Lemma §9.12 ($\mathbb{Z}_\ell^*$ is a commutative group).