Leipzig University
Institute of Computer Science
Winter Term 2020/21

Prof. Dr. Andreas Maletti
Fabian Tronicke

Cryptography

Exercise Sheet 10

will be discussed on January 26, 2021

Exercise 10.1

Assume a public-key encryption scheme $\mathcal{E} = (\text{gen}, \text{enc}, \text{dec})$ for single-bit messages with no decryption error ($\text{dec}_{k_d}(m) \neq \perp$). Let c be a ciphertext computed by $c \leftarrow \text{enc}_{k_e}(m)$ for a message m and public-key k_e. Show that an unbounded adversary could compute m with probability 1.
This means that something like 'perfectly secret' for public-key encryption schemes is not achievable.

Exercise 10.2

Let $\mathcal{E} = (\text{gen}, \text{enc}, \text{dec})$ be a public-key encryption scheme for only single-bit messages. We construct a public-key encryption scheme $\mathcal{E}' = (\text{gen}, \text{enc}', \text{dec}')$ that has message space $\{0,1\}^*$ by defining enc' as follows:

$$\text{enc}'_{k_e}(m) = \text{enc}_{k_e}(m_1) \dots \text{enc}_{k_e}(m_\ell),$$

where $m = m_1 \dots m_\ell$. Decryption is defined analogously.

(a) Show that if $\mathcal{E}$ is CPA-secure, then $\mathcal{E}'$ is also CPA-secure.

(b) Does the above hold for CCA-security?