Leipzig University
Institute of Computer Science
Winter Term 2020/21

Prof. Dr. Andreas Maletti
Fabian Tronicke

Cryptography

Exercise Sheet 5

will be discussed on December 1, 2020

Exercise 5.1

Prove the converse of Theorem §5.1. Namely, show that if G is not a pseudorandom generator then the scheme $\mathcal{E}_G$ from Construction §4.7 is not EAV-secure.

Exercise 5.2

Define 'perfectly indistinguishable' (see Definition §3.2) under a chosen-plaintext attack by adapting Definition §5.9 (CPA-secure). Show that the definition cannot be achieved.

Exercise 5.3

Let $\mathcal{E}_1 = (\mathrm{gen}_1, \mathrm{enc}_1, \mathrm{dec}_1)$ and $\mathcal{E}_2 = (\mathrm{gen}_2, \mathrm{enc}_2, \mathrm{dec}_2)$ be two private-key encryption schemes for which it is known that at least one is CPA-secure (but you don't know which). Construct a private-key encryption scheme (using $\mathcal{E}_1$ and $\mathcal{E}_2$) that is guaranteed to be CPA-secure.

Hint:

Generate two plaintext messages from the original plaintext so that knowledge of either one reveals nothing about the original plaintext, but knowledge of both enables the original plaintext to be computed.