Leipzig University
Institute of Computer Science
Winter Term 2020/21

Prof. Dr. Andreas Maletti
Fabian Tronicke

Cryptography

Exercise Sheet 6

will be discussed on December 8, 2020

Exercise 6.1

Open question from last exercise:
Let $\mathcal{E}_1 = (\text{gen}_1, \text{enc}_1, \text{dec}_1)$ and $\mathcal{E}_2 = (\text{gen}_2, \text{enc}_2, \text{dec}_2)$ be two private-key encryption schemes for which it is known that at least one is CPA-secure (but you don't know which). Is the private-key encryption scheme $\mathcal{E}_2 \circ \mathcal{E}_1 = (\text{gen}, \text{enc}, \text{dec})$, defined by

$$\begin{aligned}\text{gen}(1^n) &= (k_1, k_2) = (\text{gen}_1(1^n), \text{gen}_2(1^n))\\ \text{enc}_k(m) &= \text{enc}_{2,k_2}(\text{enc}_{1,k_1}(m))\\ \text{dec}_k(c) &= \text{dec}_{1,k_1}(\text{dec}_{2,k_2}(c))\end{aligned}$$

CPA-secure?

Exercise 6.2

Consider a stateful variant of CBC-mode encryption where the sender simply increments the i by 1 each time a message is encrypted (rather than choosing i at random each time). Show that the resulting scheme is not CPA-secure.

Exercise 6.3

What is the effect of a

(a) dropped ciphertext block (e.g., if the transmitted ciphertext $c_1, c_2, c_3, \ldots$ is received as $c_1, c_3, \ldots$)

(b) single-bit error in the ciphertext

when using the CBC, OFB and CTR modes of operation?

More precise:
Say a message $m_1, m_2, \ldots$ is encrypted to give a ciphertext $c_0, c_1, c_2, \ldots$ and then

(a) a single block c_i is dropped

(b) a single bit is flipped in c_i to give modified block c_i'.

Look at the effect of decrypting the modified ciphertext using each of the stated modes to obtain a message $m_1', m_2', \ldots$.