

Cryptography Exercise Sheet 9

Prof. Dr. Thomas Wilke, Dr.-Ing. Kim-Manuel Klein

15. Mai 2020

1. **Problem:** *AE-security: simple examples (Exercise 9.1 in BS)*

Let (E, D) be an AE-secure cipher. Consider the following derived ciphers:

$$(a) \ E_1(k, m) := (E(k, m), E(k, m)); \ D_1(k, (c_1, c_2)) := \begin{cases} D(k, c_1) & \text{if } D(k, c_1) = D(k, c_2) \\ \mathbf{reject} & \text{otherwise} \end{cases}$$

$$(b) \ E_2(k, m) := \{c \leftarrow E(k, m), \text{output}(c, c)\}; \ D_2(k, (c_1, c_2)) := \begin{cases} D(k, c_1) & \text{if } c_1 = c_2 \\ \mathbf{reject} & \text{otherwise} \end{cases}$$

Show that part (b) is AE-secure, but part (a) is not.