1. Show that one has to be very careful with modifications of CBC-MAC, small modifications can be disastrous. Exercises 4.9 and 4.8 of [KL].

2. CCA-Security: Exercise 3.22 from [KL].


4. **Different security goals should always use independent keys!** We derive an example what can go wrong if the same key is used in the Encrypt-then-Authenticate approach (which yields CCA-security if independent keys are used!).

Let $F$ be a strong pseudorandom permutation according to Definition 3.28 in [KL]. Let the key $k \leftarrow \{0,1\}^n$ be picked uniformly at random by $\text{Gen}$. Define $\text{Enc}_k(m) = F_k(m||r)$ for $m \in \{0,1\}^{n/2}$ and a random $r \leftarrow \{0,1\}^{n/2}$, and define $\text{Mac}_k(c) = F_k^{-1}(c)$.

(a) Define the corresponding decryption function $\text{Dec}_k(\cdot)$ and prove that this encryption scheme $(\text{Gen, Enc, Dec})$ is CPA-secure.

(b) Prove that the authentication code is a secure MAC.

(c) Conclude that the combination of the two schemes in the Encrypt-then-Authenticate approach using the same key $k$ is completely insecure.

Who might have sent this message?

Image credit: https://secure.flickr.com/photos/susanneg/262987063/.