Exercise 19. Construct a forged MAC for the CBC-MAC algorithm from ex. 10.5 in the lecture notes. Assume the attacker has knowledge of two text-MAC pairs and their respective initial values $C_0$.

Propose a countermeasure against this attack.

Exercise 20.

In the verification step of the ElGamal-Signature one first checks, whether $1 \leq r < p$. Show that an attacker can generate a signature for an arbitrary message $m'$ by intercepting one valid signature $(r, s)$ for a message $m$ if this step is omitted.

Hint: Assume that $h(m)$ is invertible modulo $p - 1$.

Exercise 21. Let $p$ prime, $p \equiv 3 \pmod{4}$, and $a$ a primitive root modulo $p$. Furthermore, let $y \equiv a^x \pmod{p}$ a public ElGamal key and let $a \mid p - 1$.

Assume that it is possible to find $z \in \mathbb{Z}$ such that $a^{rz} \equiv y^r \pmod{p}$.

Show that $(r, s)$ with

$$s = \frac{p - 3}{2}(h(m) - rz)$$

is a valid ElGamal signature for a chosen message $m$. 