Übung 1

Aufgabe 2a)

geg: $M = \mathbb{Z}_{26}^{\ell}$ $\ell \in \mathbb{N}$

$K = \mathbb{Z}_{26}$

$C = M$

Gen: Setze $k \leftarrow K$, Gib k

Enc: ~~Für~~ für $k \in K$ und $m = m_0 \dots m_{l-1}$
setze $c_i := (m_i + k) \bmod 26$

Dec = ?

Dec: ~~Für~~ für $k \in K$ und [redacted] $c = c_0 \dots c_{l-1}$

Setze $m_i := (c_i - k) \bmod 26$

gib $m = m_0 \dots m_{l-1}$ aus