4.3.2020

Übung 1, -

Aufgabe 1, -

Korrektheit der Vigenère Chiffre:

- Gen: $k = k_0 \dots k_{t-1} \leftarrow \mathbb{Z}_{26}^t$
- Enc: bei $k = k_0 \dots k_{t-1}$ und $m = m_0 \dots m_{l-1}$

  gib $c = c_0 c_1 \dots c_{l-1}$, $\boxed{c_i = m_i + k_i \bmod t \bmod 26}$
- Dec: bei $k = k_0 \dots k_{t-1}$ und $c = c_0 \dots c_{l-1}$

  gib $m = m_0 \dots m_{l-1}$, $\boxed{m_i = c_i - k_i \bmod t \bmod 26}$

$$Dec(Enc(m)) = m$$

$$= Dec(m_0 + k_0 \bmod t \dots m_{l-1} + k_{l-1} \bmod t) = m$$

$$= m_0 + k_0 \bmod t - k_0 \bmod t \dots m_{l-1} + k_{l-1} \bmod t - k_{l-1} \bmod t = m$$

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

$m = m$ ✓ w.A.