3)

a)

provide m^i and calculate $H(m^i)$.

$k = H\left(m^i\right) \oplus MAC_K(m^i)$

Since key is retrieved, MAC is insecure

b) is secure

c)

represent $m = m_1\left|\right|m_2\left|\right|...||m_n||b$, $MAC_k(m) = H(k\left|\right|m_1\left|\right|m_2\left|\right|...\left|\right|m_n|\left|b\right) \oplus$
$H(m_1\left|\right|m_2\left|\right| ... ||m_n||b)$

provide m^1 , receive $MAC_K(m^1)$

Conduct a length extension attack where $m' = m\left|\right|m_{n+1}\left|\right|b$

Discussed with Sean, Louis, Min Htet, Min Yue