M343L: HOMEWORK SET 8 PROOFS

ANDREW TSENG: ART2589

Problem 6.17

Part a:
To prove $m_1' = m_1, m_2' = m_2$.
Proof: We know that $S = n_1 R = T$ where $S = kQ_a, R = kP$ which makes shows that the pairing will lead to

$$x_T^{-1} x_S m_1 = m_1' = m_1$$
$$y_T^{-1} y_S m_2 = m_2' = m_2$$

Part b:

Problem 6.18

Problem 6.29

Problem 6.32

Problem 6.33