Prob 44

$$k \stackrel{?}{=} \frac{(H(m_1) - H(m_2))}{(s_1 - s_2)} \bmod q$$

$$= (H(m_1) - H(m_2))(s_1 - s_2)^{-1} \bmod q$$

$$s_i = k^{-1}(H(m_i) + xr) \bmod q$$

$$r = (g^k \bmod p) \bmod q$$

~~$s_1 - s_2 = k^{-1}(H(m_1) + xr) \bmod q - k^{-1}(H(m_2) + xr) \bmod q$~~

$$= [(H(m_1) - H(m_2)) \bmod q][\underbrace{(s_1 - s_2)^{-1} \bmod q}] \bmod q$$

$$[(s_1 - s_2) \bmod q]^{-1} \bmod q$$

$$(s_1 - s_2) \bmod q = [k^{-1}(H(m_1) + xr) \bmod q - k^{-1}(H(m_2) + xr) \bmod q] \bmod q$$

$$= [k^{-1}H(m_1) + \cancel{k^{-1}xr} - k^{-1}H(m_2) - \cancel{k^{-1}xr}] \bmod q$$

$$= k^{-1}(H(m_1) - H(m_2)) \bmod q$$

$$k \stackrel{?}{=} [(H(m_1) - H(m_2)) \bmod q]\{[\underbrace{k^{-1}(H(m_1) - H(m_2)) \bmod q}]^{-1} \bmod q\} \bmod q$$

$$k(H(m_1) - H(m_2))^{-1} \bmod q$$

$$= (\cancel{H(m_1) - H(m_2)})\, k\, (\cancel{H(m_1) - H(m_2)})^{-1} \bmod q$$

$$k \stackrel{\checkmark}{=} k \bmod q$$