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:
The message given from MV-elgamal encryption is (R, c_1, c_2)

Part C:
Alice Encryption Key: $Q_A = (1104, 492)$. $(m_1, m_2) = (509, 980)$

Problem 6.18

Part A: Since Eve knows E and we know that $c_1 = x_P m_1, c_2 = y_P m_2$, thus $x_P = \frac{c_1}{m_1}, y_P = \frac{c_2}{m_2}$. Plugging these values into the curve:

$$(\frac{c_2}{m_2})^2 = (\frac{c_1}{m_1})^3 + A(\frac{c_1}{m_1}) + B$$

Eve then can solve for the roots of this polynomials for m_1 or m_2, given she knows oen of these values. It becomes as simple as solve for the roots.

Part B: Since $\frac{814}{1050} \in F_{1201} = 957$ Given the previous E, we can find two possible solutions to

$$y_s^2 = (957)^3 + 19(957) + 17$$

$y \in [182, 1019]$
If $y = 182$, then the message pair is (1050,440). If $y = 1019$, then the message pair is (1050, 761).

Problem 6.29

Proof: Given $R(x), S(x)$ are rational functions Since $div(f) = \sum_Z ord(f)Z$, then due to the additive properties of the functions at the points of the curve, we can say that

$$div(R(x)S(x)) = div(R(x)) + div(S(X))$$

Problem 6.32

Problem 6.33