

Om Khadka, U518017771

(This is a continuation of problem 3B, since my latex broke for some reason).

The last equality follows because $\Pr[Enc(K_2, m) = c_2] = \mathcal{D}(c_2)$ by OTS.

Thus, the distribution of (C_1, C_2) is the product distribution $D \times D$ which does not depend on the msg m . Consequently, this means that for any two msgs $m_0, m_1 \in M$, the distributions of $Enc_{new}((K_1, K_2), m_0)$ and $Enc_{new}((K_1, K_2), m_1)$ are identical. This proves that Enc_{new} has OTS.