Question 1. Marks: 6.0

Consider the Vigenere cipher over the lowercase English alphabet, where the key can have length 1 or length 2, each with 0.5 probability. Let the distribution over plaintexts be $Pr[M = \text{“}aa\text{”}] = 0.4$ and $Pr[M = \text{“}ab\text{”}] = 0.6$. What is $Pr[M = \text{“}aa\text{”} | C = \text{“}bb\text{”}]$? You do not have to simplify the answer to decimal places, simplify as much as you can. Please answer with detailed steps.

Question 2. Marks: 2.0

Prove or refute: An encryption scheme with message space $\mathcal{M}$ is perfectly secret if and only if for every probability distribution over $\mathcal{M}$ and every $c_0, c_1 \in \mathcal{C}$ we have $Pr[C = c_0] = Pr[C = c_1]$.

Question 3. Marks: 2.0

Prove or refute: For every perfectly secret encryption scheme it holds that for every distribution on the message space $\mathcal{M}$, every $m, m' \in \mathcal{M}$, and every $c \in \mathcal{C}$:
$Pr[M = m | C = c] = Pr[M = m' | C = c]$.