Cryptography—ENEE/CMSC/MATH 456
Class Exercise 1/29/2024

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

2. Prove or refute: An encryption scheme with message space $\boldsymbol{M}$ is perfectly secret if and only if for every probability distribution over $\boldsymbol{M}$, every $m, m' \in \boldsymbol{M}$ and every $c \in \boldsymbol{C}$ we have $Pr[M = m \mid C = c] = Pr[M = m' | C = c]$.