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

Given encryption scheme $(Gen, Enc, Dec)$, construct scheme $(Gen, Enc', Dec')$. This is exactly the same except Enc appends a 0 to its output with prob. $\frac{1}{4}$ and a 1 with prob $\frac{3}{4}$. Dec' ignores the final bit.

Note that if $(Gen, Enc, Dec)$ is perfectly secure, so is $(Gen, Enc', Dec')$. But now choose any $c \in C$ where $C$ is ciphertext space of $(Gen, Enc, Dec)$.

Then we have $Pr[C = c \mid 0] < Pr[C = c \mid 1]$.

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

Given any perfectly secret encryption scheme, we will choose a distribution over $M$ and $m, m', c$ s.t. $Pr[M = m \mid C = c] \neq Pr[M = m' \mid C = c]$. This refutes the above.

Let's choose a distribution over $M$ that sets $Pr[M = m] > Pr[M = m']$ for some $m, m'$.

Now by Def. 1 of perfect secrecy, we have

$Pr[M = m \mid C = c] = Pr[M = m]$ and $Pr[M = m' \mid C = c] = Pr[M = m']$

So $Pr[M = m \mid C = c] > Pr[M = m'] = Pr[M = m' \mid C = c]$.

So $Pr[M = m \mid C = c] \neq Pr[M = m' \mid C = c]$. 