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 $Pr[C = c_0] = Pr[C = c_1]$. \textbf{False}.

Consider the following slight modification of OTP:

Key Gen: Choose $K \in \{0,1\}^k$, choose $b = 0$ w/prob $\frac{1}{4}$ and $1$ w/prob $\frac{3}{4}$

Enc$_{K \oplus b}(m) : m \in \{0,1\}^k$, output $c \parallel b = m \oplus K \parallel b$.

Dec$_{K \oplus b}(c \parallel b)$: output $m = c \oplus K$.

Above is still perfectly secret (you show this $\diamond$).

But now, choose any $c \in \{0,1\}^k$ and consider

\[ Pr[c \parallel 0 = c \parallel 0] = Pr[C = c], \quad Pr[B = 0] = Pr[C = c] \cdot \frac{1}{4} \]
\[ Pr[c \parallel 1 = c \parallel 1] = Pr[C = c] \cdot Pr[B = 1] = Pr[C = c] \cdot \frac{3}{4} \]

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

$Pr[M = m | C = c] = Pr[M = m' | C = c]$. \textbf{False}.

Given any perfectly secret encryption scheme, we choose a distribution over $\emptyset$ $\emptyset$ and $m, m', c$ s.t.

$Pr[M = m | C = c] \neq Pr[M = m' | C = c]$. This refutes the above.

We choose a distribution over $\emptyset$ $\emptyset$ that sets $Pr[M = m] > Pr[M = m']$ for some $m, m'$.

Now by Def 1 of perfect secrecy $\forall C$:

$Pr[M = m | C = c] = Pr[M = m]$ and $Pr[M = m' | C = c] = Pr[M = m']$.

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

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