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.**

Consider the following slight modification of OTP:

Key Gen: Choose $k \xleftarrow{R} \{0,1\}^\ell$, Choose $b = 0$ w/ prob $\frac{1}{4}$ and 1 w/ prob $\frac{3}{4}$

$Enc_{k\|b}(m)$: $m \in \{0,1\}^\ell$. output ~~$m \oplus$~~ $c\|b = m \oplus k \| b$.

$Dec_{k\|b}(c\|b)$: output $m := c \oplus k$.

Above is still perfectly secret (→ Show this & at).

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

$$Pr[C\|B = c\|0] = Pr[C=c] \cdot Pr[B=0] = Pr[C=c] \cdot \frac{1}{4}$$

$\neq$

$$Pr[C\|B = c\|1] = Pr[C=c] \cdot Pr[B=1] = Pr[C=c] \cdot \frac{3}{4}$$

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 $Pr[M = m \mid C = c] = Pr[M = m'|C = c]$. **False.**

Given any perfectly secret encryption scheme, we 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.

We choose a distribution over M that sets

$$Pr[M=m] > Pr[M=m'] \text{ for some } m, m'.$$

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

$$Pr[M=m \mid C=c] = Pr[M=m] \text{ and } Pr[M=m'|C=c] = Pr[M=m']$$

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

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