Introduction to Cryptology—ENEE 459E/CMSC 498R
Class Exercise 2/2/17

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 $Pr[C = c_0] = Pr[C = c_1]$.

Consider the following scheme
Message space is a single letter $\mathcal{M} = \{A, B, C \dots\}$

$\boxed{\begin{array}{l} \text{Gen() - choose a shift } s \xleftarrow{R} \{0, \dots 25\} \\ \quad \text{- choose } r \text{ to be the letter A with prob } 3/4\text{, B with prob } 1/4 \\ \text{Enc}(s\|r, m) \text{ - apply shift cipher to } m \text{ w/ shift } s \text{ yielding } c \\ \quad \text{output } c\|r \\ \text{Dec}(s\|r, c\|r) \text{ - decrypt shift cipher w/ } c, s \text{ yielding } m \end{array}}$

It can be observed that above achieves perfect secrecy.
However, ciphertexts ending in <u>A</u> are more likely than ciphertexts ending with <u>B</u>.

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

Assume an encryption scheme is perfectly secret and for every dist over $\mathcal{M}$, every $m, m' \in \mathcal{M}$, $c \in \mathcal{C}$ we have $Pr[M=m \mid C=c] = Pr[M=m' \mid C=c]$.
Let's choose a particular distribution over $\mathcal{M}$ that sets $Pr[M=m] > Pr[M=m']$.
Now by Def 1 of perfect secrecy
$Pr[M=m \mid C=c] = Pr[M=m] = Pr[M=m' \mid C=c] = Pr[M=m']$.
But this implies $Pr[M=m] = Pr[M=m']$, which is a contradiction.