Solutions

Cryptography—ENEE/CMSC/MATH 456
Class Exercise 2/3/20

1. Prove or refute: An encryption scheme with message space $\mathcal{M}$ is perfectly secret if and only if for every probability distribution over $\mathcal{M}$ and every $c_0, c_1 \in \mathcal{C}$ 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 $1/4$ and 1 w/ prob $3/4$

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

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

Above is still perfectly secret [** Show this **].

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

$$Pr[C\|B = c\|0] = Pr[C=c] \cdot Pr[B=0] = Pr[C=c] \cdot 1/4$$
$$\neq$$
$$Pr[C\|B = c\|1] = Pr[C=c] \cdot Pr[B=1] = Pr[C=c] \cdot 3/4$$

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

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

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

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

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

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

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