Week 9 : Theory Solutions

1. Say the key space consists of N keys. The proceeds as follows:

$$\begin{aligned}
\Pr[M = m | C = c] &= \frac{\Pr[M = m \cdot C = c]}{\Pr[C = c]} \\
&= \frac{\Pr[K = m \oplus c] \cdot \Pr[M = m]}{\sum_k \Pr[M = c \oplus k] \cdot \Pr[K = k]} \\
&= \frac{\frac{1}{N} \cdot \Pr[M = m]}{\frac{1}{N} \sum_k \Pr[M = k \oplus c]} \\
&= Pr[M = m] \qquad \left(\because \sum_k \Pr[M = k \oplus c] = 1 \right)
\end{aligned}$$

2. By way of contradiction say, $|\mathcal{K}| < |\mathcal{M}|$. Let us define $\mathcal{M}(c) = \{m \,|\, m = \text{Dec}_k(c) \text{ for some } k \in \mathcal{K}\}$. Clearly $|\,\mathcal{M}(c)| \leq |\mathcal{K}|$. But, $||\mathcal{K}| < |\mathcal{M}|$. Therefore, $|\,\mathcal{M}(c)| < |\mathcal{M}|$. There must exist some $m' \in \mathcal{M}$ such that $m' \notin \mathcal{M}(c)$. Therefore,

$$\Pr[M = m' \,|\, C = c] = 0 \neq \Pr[M = m'].$$

   This is a contradiction.

3. Probability must be conditioned on events when Eve chooses the correct basis and when Eve chooses the wrong basis. Each of these events must further be conditioned on Bob's choice of basis.

4. Compute inner product.

5. One time pad along with quantum key distribution would only solve the problem of confidentiality, which is what most people associate cryptography with. However, the scope of cryptography goes far beyond just confidentiality and is also concerned with properties such integrity, authenticity and non-repudiation. The reader is recommended to look up these term in some standard cryptography text, to get a more holistic view of cryptography.