COMP6453 Assignment I

June 25, 2025

Recall the definition of perfect secrecy, is that the presence of the ciphertext c does not reveal information about the plain text m meaning that

$$P(M = m|C = c) = P(M = m) \tag{1a}$$

and $m \in M$ $c \in C$ and $k \in K$. Where M, K, C are their respective spaces.

This also implies by Bayes Theorem that:

$$P(C = c|M = m) * P(M = m) = P(M = m|C = c) * P(C = c) \tag{2a}$$

Because $P(M = m) > 0$ and $P(C = c) > 0$ and this implies: $P(C = c|M = m) = P(C = c)$(2b).

For some encryption scheme with E, for it to be considered perfectly secret, it must be shown that it is uniformly distributed over M,C with Key Space K, for any message $m \in M$ and any cipher text $c \in C$;

Then every $P(M = m) > 0$ and $P(C = c) > 0$ and that $E(k, m_0) = c_0$ and $E(k, m_1) = c_0$ for $k \in K$.

$$\begin{aligned} P(C = c|M = m) &= P(E(k, M) = c|M = m) && \text{(3a)} \\ &= P(E(k, m) = c|M = m) && \text{(3b)} \\ &= P(E(k, m) = c) && \text{(3c)} \end{aligned}$$

3a) is by defintion the encryption of m that is $E(k, m) = c$. 3b) is because we condition on the event that some plaintext $M = m_0$ Then it 3c) occurs because the key k is independent from the message space where $M = m$

Therfore, using equation 2b), 3c) and $m_0, m_1 \in M$:

$$\begin{aligned} P(E(k, m_0) = c) &= P(C = c|M = m_0) && \text{(4a)} \\ &= P(C = c) && \text{(4b)} \\ &= P(C = c|M = m_1) = P(E(k, m_0) = c) && \text{(4c)} \end{aligned}$$

So when $P(E(k, m_0) = c)$ and $P(E(k, m_1) = c)$ for some c. This means when $E(k, m_1) = c_1$ and $E(k, m_0) = c_0$ then $P(E(k, m_0) = c_0) = P(E(k, m_1) = c_1)$.

Therefore $P(C = c_0) = P(C = c_1)$. Thus the encryption mechanism provided has perfect secrecy. QED.