1. Prove that, by redefining the key space, we may assume the key-generation algorithm Gen chooses a key uniformly at random, without changing \( \Pr[C = c | M = m] \) for any \( m, c \).

**Hint:** Define the key space to be the set of all possible random tapes for the randomized algorithm \( \text{Gen} \).

2. Prove or refute: An encryption scheme with message space \( \mathcal{M} \) is perfectly secret if and only if for every probability distribution over \( \mathcal{M} \) and every \( c_0, c_1 \in \mathcal{C} \) we have \( \Pr[C = c_0] = \Pr[C = c_1] \).

3. In this problem we consider definitions of perfect secrecy for the encryption of two messages (using the same key). Here we consider distributions over pairs of messages from the message space \( \mathcal{M} \); we let \( M_1, M_2 \) be random variables denoting the first and second message, respectively. We generate a (single) key \( k \), sample messages \((m_1, m_2)\) according to the given distribution, and then compute ciphertexts \( c_1 \leftarrow \text{Enc}_k(m_1) \) and \( c_2 \leftarrow \text{Enc}_k(m_2) \); this induces a distribution over pairs of ciphertexts and we let \( C_1, C_2 \) be the corresponding random variables.

(a) Say encryption scheme \((\text{Gen}, \text{Enc}, \text{Dec})\) is perfectly secret for two messages if for all distributions over \( \mathcal{M} \times \mathcal{M} \), all \( m_1, m_2 \in \mathcal{M} \), and all ciphertexts \( c_1, c_2 \in \mathcal{C} \) with \( \Pr[C_1 = c_1 \land C_2 = c_2] > 0 \):

\[
\Pr[M_1 = m_1 \land M_2 = m_2 | C_1 = c_1 \land C_2 = c_2] = \Pr[M_1 = m_1 \land M_2 = m_2].
\]

Prove that no encryption scheme can satisfy this definition.

**Hint:** Take \( m_1 \neq m_2 \) but \( c_1 = c_2 \).

(b) Say encryption scheme \((\text{Gen}, \text{Enc}, \text{Dec})\) is perfectly secret for two distinct messages if for all distributions over \( \mathcal{M} \times \mathcal{M} \) where the first and second messages are guaranteed to be different (i.e., distributions over pairs of distinct messages), all \( m_1, m_2 \in \mathcal{M} \), and all \( c_1, c_2 \in \mathcal{C} \) with \( \Pr[C_1 = c_1 \land C_2 = c_2] > 0 \):

\[
\Pr[M_1 = m_1 \land M_2 = m_2 | C_1 = c_1 \land C_2 = c_2] = \Pr[M_1 = m_1 \land M_2 = m_2].
\]

Show an encryption scheme that provably satisfies this definition.

**Hint:** The encryption scheme you propose need not be efficient, though an efficient solution is possible.

4. When using the one-time pad with the key \( k = 0^\ell \), we have \( \text{Enc}_k(m) = k \oplus m = m \) and the message is sent in the clear! It has therefore been suggested to modify the one-time pad by only encrypting with \( k \neq 0^\ell \) (i.e., to have \( \text{Gen} \) choose \( k \) uniformly at random from the set of non-zero keys of length \( \ell \)). Is this modified scheme still perfectly secret? Explain.