2.1 Prove the second direction of Lemma 2.2.

2.2 Prove or refute: For every encryption scheme that is perfectly secret it holds that for every distribution over the message space $\mathcal{M}$, every $m, m' \in \mathcal{M}$, and every $c \in \mathcal{C}$:

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

2.3 When using the one-time pad (Vernam's cipher) with the key $k = 0^\ell$, it follows that $\mathsf{Enc}_k(m) = k \oplus m = m$ and the message is effectively sent in the clear! It has therefore been suggested to improve the one-time pad by only encrypting with a key $k \neq 0^\ell$ (i.e., to have Gen choose $k$ uniformly at random from the set of *non-zero* keys of length $\ell$). Is this an improvement? In particular, is it still perfectly secret? Prove your answer. If your answer is positive, explain why the one-time pad is not described in this way. If your answer is negative, reconcile this with the fact that encrypting with $0^\ell$ doesn't change the plaintext.

2.5 Prove or refute: Every encryption scheme for which the size of the key space equals the size of the message space, and for which the key is chosen uniformly from the key space, is perfectly secret.

***LEMMA 2.2*** *An encryption scheme* (Gen, Enc, Dec) *over a message space $\mathcal{M}$ is perfectly secret if and only if for every probability distribution over $\mathcal{M}$, every message $m \in \mathcal{M}$, and every ciphertext $c \in \mathcal{C}$:*

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

**PROOF** Fix a distribution over $\mathcal{M}$ and arbitrary $m \in \mathcal{M}$ and $c \in \mathcal{C}$. Say

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

Multiplying both sides of the equation by $\Pr[M = m] / \Pr[C = c]$ gives

$$\frac{\Pr[C = c \mid M = m] \cdot \Pr[M = m]}{\Pr[C = c]} = \Pr[M = m].$$

Using Bayes' theorem (see Theorem A.8), the left-hand-side is exactly equal to $\Pr[M = m \mid C = c]$. Thus, $\Pr[M = m \mid C = c] = \Pr[M = m]$ and the scheme is perfectly secret.

The other direction of the proof is left as an exercise. ∎