1 Substitution cipher [15 points]

Have a look at the substitution cipher in Lecture Notes 1 (section 3.2) and recall the definition of perfect secrecy. Prove that the substitution cipher is perfectly secure for the special case of $\ell = 1$, and that it is not perfectly secure if $\ell \geq 2$.

2 OTP cipher variations [30 points]

We showed that One-Time Pad encryption satisfies perfect secrecy if $\mathcal{M} = \mathcal{K} = \{0, 1\}^\ell$, for any $\ell$. Consider some variations of the OTP cipher, where the messages and/or keys are binary strings as before but with some strings missing. Consider set $\mathcal{S}$ of three 2-bit strings, $\mathcal{S} = \{00, 01, 10\}$.

Consider the following three variations on the OTP cipher. In all these variations the key generation algorithm chooses $k \in \mathcal{K}$ uniformly, and encryption and decryption work as in OTP, i.e. $\text{Enc}(k, m) = k \oplus m$ and $\text{Dec}(k, c) = k \oplus c$.

For each of the OTP variations below, say whether the resulting cipher is perfectly secure or not, and prove your answer. In each case, say what the space $\mathcal{C}$ of the ciphertexts is, and note the sizes of the message space $\mathcal{M}$ and key space $\mathcal{K}$. Do these sizes correlate somehow with whether or not the cipher is secure? Can you explain why?

1. Let $\mathcal{M} = \mathcal{S}^\ell$ and $\mathcal{K} = \{0, 1\}^{2\ell}$, i.e. both the message and the key are $(2\ell)$-long bit strings. However, not every $(2\ell)$-bit string can be a valid message. For example, for $\ell = 3$, we could have $m = [00, 01, 00] = 000100$ but $m = [11, 00, 11] = 110011$ is not in $\mathcal{M}$ because $11 \notin \mathcal{S}$.

2. Let $\mathcal{M} = \{0, 1\}^{2\ell}$ and $\mathcal{K} = \mathcal{S}^\ell$

3. Let $\mathcal{M} = \mathcal{K} = \mathcal{S}^\ell$. [[Hint: This one is actually not perfectly secure...]]

\[1\]We use notation $\mathcal{A}^n$ to denote a set of $n$-long sequences $[A_1, A_2, ..., A_n]$ where each $A_i$ is an element of $\mathcal{A}$. Using this notation, $\{0, 1\}^n$ denotes a set of all $n$-long binary strings.