1 Substitution cipher

Have a look at the substitution cipher in Lecture Notes 1 (section 3.3) 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

Notation: We will denote by $A^n$ a set of $n$-long sequences of symbols $A_1A_2\ldots A_n$ where each $A_i$ is an element of $A$. For example, taking $A = \{0, 1\}$, we will write $\{0, 1\}^n$ to denote a set of all $n$-long binary strings.

We showed that One-Time Pad encryption satisfies perfect secrecy if $M = K = \{0, 1\}^\ell$, for any $\ell$. In this exercise we will look at variations of the OTP cipher, where the messages and/or keys are not any binary strings. For example, consider set $S$ of three 2-bit strings, $S = \{00, 01, 10\}$.

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

Consider the following three OTP variants:

1. Let $M = S^\ell$ and $K = \{0, 1\}^{2\ell}$. In this way both the message and the key are $(2\ell)$-long bit strings, but 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 $M$ because $11 \notin S$.

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

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

For each of these OTP variants do the following: (1) Say what the space $C$ of the ciphertexts is, and note the sizes of the message space $M$ and key space $K$; and (2) Say whether the resulting cipher is perfectly secure or not, and prove your answer.

Do the sizes of the key space and the message space correlate in any way with whether or not the cipher is secure? Explain how and why.

3 Perfect Secrecy implies Shannon Secrecy [bonus]

Prove that if an encryption scheme is perfectly secret than it must also be secret in Shannon’s sense.