Example exercise 1 - Shannon's theory of secrecy

Let $\mathbf{M}$ be the plaintext, K the key, and $\mathbf{C}$ the ciphertext ni some arbitrary cryptosystem.

- Show that
$$0 \leq H(\mathbf{M}|\mathbf{C}) \leq H(K|\mathbf{C}).$$
- Give an example of a cryptosystem where
$$0 < H(\mathbf{M}|\mathbf{C}) < H(K|\mathbf{C}).$$
- Give an example of a cryptosystem where
$$0 < H(\mathbf{M}|\mathbf{C}) = H(K|\mathbf{C}).$$

Example exercise 2 - Shannon's theory of secrecy

Assume a source with output symbols A, B, C, D, where $P(A) = 1/2$, $P(B) = 1/4$, $P(C) = P(D) = 1/8$. Output symbols are chosen independently.

- Determine the unicity distance if the source is encrypted by a simple substitution cipher.
- To increase the unicity distance, explain how homophonic coding can be used.