Exercise 1 (multiplicative one-time pad).

We may also define a "multiplication $\bmod p$" variation of the one-time pad. This is a cipher $\mathcal{E} = (E, D)$, defined over (K, M, C), where

$$K := M := C := \{1, \ldots, p-1\},$$

where p is a prime. Encryption and decryption are defined as follows:

$$E(k, m) := k \cdot m \bmod p \quad ; \quad D(k, c) := k^{-1} \cdot c \bmod p.$$

Here, k^{-1} denotes the multiplicative inverse of k modulo p. Verify the correctness property for this cipher and prove that it is perfectly secure.

Exercise 2 (Chain encryption).

Let $\mathcal{E} = (E, D)$ be a perfectly secure cipher defined over (K, M, C) where $K = M$. Let $\mathcal{E}' = (E', D')$ be a cipher where encryption is defined as

$$E'(\ (k_1, k_2),\ m) := \ \big(E(k_1, k_2),\ E(k_2, m)\big)\ .$$

Show that $\mathcal{E}'$ is perfectly secure.