1. For each one of the following MAC schemes, either prove that they are secure (in the sense defined in class, namely EU-CMA), or provide a counter example to their security. Unless said otherwise, the verification algorithm works by re-computing the tag and comparing to the received tag: \( \text{VER}(k, m, t) = \text{accept iff } \text{AUTH}(k, m) = t \).

(a) \([30 \text{ pt}]\) Let \((\text{ENC}, \text{DEC})\) be a CPA-secure encryption scheme. Then \(\text{AUTH}(k, m) = m, \text{ENC}(k, m)\), and \(\text{VER}(k, m, t) = \text{accept iff } \text{DEC}(k, t) = m\).

(b) \([30 \text{ pt}]\) Let \(F = \{F^n\}_{n \in \mathbb{N}}, F^n = \{F_k : \{0, 1\}^n \rightarrow \{0, 1\}^n\}_{k \in \{0, 1\}^n}\) be a PRF ensemble, and let \(f\) be a one way function. Then, \(\text{AUTH}(k, m) = m, f(F_k(m))\).

2. \([60 \text{ points}]\) Let \(F = \{F^n\}_{n \in \mathbb{N}}, F^n = \{F_k : \{0, 1\}^{2n} \rightarrow \{0, 1\}^{2n}\}_{k \in \{0, 1\}^n}\) be a PRP ensemble. Consider the following shared key encryption scheme for message space \(M_n = \{0, 1\}^n\):

- For \(m \in \{0, 1\}^n, \text{ENC}(k, m) = f_k(m \circ r)\), where \(r \leftarrow U_n\). (Here \(\circ\) denotes concatenation.)
- \(\text{DEC}(k, c)\) outputs the first \(n\) bits of \(f_k^{-1}(c)\).

Is \((\text{ENC}, \text{DEC})\) CPA secure, with respect to message space \(M\) and leakage function \(l(m) = |n|\)? Either prove based on the assumption that the underlying ensemble \(F\) is a PRF, or provide a counter example.