1. In class, we defined two different notions of MAC security.

**Strong unforgeability.** In this attack game, the adversary makes a series of queries, \(m_1, \ldots, m_q\) to the challenger. For query \(i\), the challenger responds to \(m_i\) with \(t_i \leftarrow \text{Mac}_k(m_i)\). Finally, the adversary submits a pair \((\hat{m}, \hat{t})\) to the challenger, and the adversary wins the game if \(\text{Vrfy}_k(\hat{m}, \hat{t}) = 1\) and \((\hat{m}, \hat{t}) \notin \{(m_i, t_i) : i = 1, \ldots, q\}\).

**Full interactive security.** In this attack game, the adversary makes a sequence of queries to the challenger. There are two types of queries: a “signing query” \((\text{sign}, m)\), to which the challenger responds with \(\text{Mac}_k(m)\), and a “verify query” \((\text{verify}, \hat{m}, \hat{t})\), to which the challenger responds with \(\text{Vrfy}_k(\hat{m}, \hat{t})\). The adversary wins the game if the adversary submits a verify query with message \(\hat{m}\) which yields a response of 1, and \(\hat{m}\) is not equal to any of the \(m_i\)'s submitted in previous signing queries.

(a) Prove that strong unforgeability implies full interactive security. This is a bit tricky.

Hint: start with an adversary \(A\) that wins the full interactive security game with some non-negligible probability \(\epsilon\), and design an adversary \(B\) that wins the strong unforgeability game with probability \(\epsilon/q\) (which is also non-negligible). Adversary \(B\) will use \(A\) as a subroutine, but will have to “guess” in advance the first query that makes \(A\) win.

(b) Prove that full interactive security does not imply strong unforgeability. This is pretty easy.

2. Let \(X, Y, K\) be finite sets, and let \(H := \{H_k\}_{k \in K}\) be a family of functions \(H_k : X \to Y\). Assume that given \(k\) and \(x\), we can efficiently compute \(H_k(x)\).

We assume that \(H\) is **weakly collision resistant**, which means that every efficient adversary wins the following attack game with negligible probability:

- The adversary chooses \(x, x' \in X\), and sends \(x, x'\) to the challenger.
- The challenger chooses \(k \in K\) at random, and evaluates \(y = F_k(x)\) and \(y' = F_k(x')\). The adversary wins if \(y = y'\) but \(x \neq x'\).

Let \(\{F_{k'}\}_{k' \in K'}\) be a pseudo-random family of functions \(F_{k'} : Y \to Z\). For \(k \in K\), \(k' \in K'\), and \(x \in X\), define \(F_{(k,k')}(x) := F_{k'}(H_k(x))\), so that each \(F_{(k,k')}\) is a function from \(X\) to \(Z\).

Now consider the family of functions \(\{F_{(k,k')}\}_{(k,k') \in K \times K'}\). Show that this is a pseudo-random family of functions.

Note that a random key for this function family is generated by choosing \(k \in K\) and \(k' \in K'\) at random, and the key is the pair \((k, k')\).

Hint: try using a “sequence of games” argument, using the Difference Lemma, as we did in class.

3. The previous exercise gives us a way to extend the domain of a PRF, assuming we have a weakly collision resistant family of functions that map long inputs to short outputs. This exercise illustrates a simple construction of such a family of functions, which maps inputs to outputs that are about half as long.
Let $p$ be a large prime (say $p \approx 2^{128}$), and let $\mathcal{I}_p := \{0, \ldots, p - 1\}$. Let $\mathcal{K} := \mathcal{I}_p$ and $\mathcal{X} := \mathcal{I}_p \times \mathcal{I}_p$. For $k \in \mathcal{K}$ and $(x_1, x_2) \in \mathcal{X}$, define $H_k(x_1, x_2) := (x_1k + x_2) \mod p \in \mathcal{I}_p$.

Prove that $\{H_k\}_{k \in \mathcal{K}}$ is weakly collision resistant. In particular, no adversary (no matter how powerful) can win the attack game with probability better than $1/p$. 