Note: In the UF-CMA definition (whether for strong or weak), an adversary’s forgery must be one of its verification queries. Also, recall that a message authentication code is a special kind of a message authentication scheme, where $T$ is deterministic and stateless and $V$ is canonical — namely, $V$ re-computes the tag of the input message and checks that it matches the input tag. We do not distinguish between weak and strong UF-CMA for message authentication codes, because they mean the same thing in this case (you should verify this as an exercise for yourself).

Exercise 1. (50 points.) Prove the following theorem.

**Theorem 1.** Let $\text{MAC} = (K, T, V)$ be a message authentication code. Suppose there is a UF-CMA adversary $A$ against $\text{MAC}$ making at most $q_t$ tagging queries and $q_v$ verification queries. Then there is a UF-CMA adversary $B$ against $\text{MAC}$ making at most $q_t$ tagging queries and one verification query such that

$$\text{Adv}_{\text{MAC}}^{\text{uf-cma}}(A) \leq q_v \cdot \text{Adv}_{\text{MAC}}^{\text{uf-cma}}(B).$$

Furthermore, the running-time of $B$ is that of $A$ plus small overhead.

What is the practical interpretation of the theorem?

Exercise 2. (100 points.) Let $\text{MAC} = (K, T, V)$ be a UF-CMA secure message authentication code. Show how to modify $\text{MAC}$ into a message authentication scheme $\text{MA}$ such that:

- $\text{MA}$ is weakly UF-CMA secure against adversaries making at most one verification query. You must state and prove a theorem for this in the style of Theorem 1.

- There is a “reasonable” UF-CMA adversary against $\text{MA}$ making many verification queries whose weak UF-CMA advantage is 1. The fewer queries your adversary makes, the more points you get. The best attack I’m aware of makes about $k$ verification queries, where $k$ is the key-length of $\text{MAC}$.

Note that such a modification is not possible if $\text{MA}$ is required to be a message authentication code. Why not?