Cryptography: Homework 7

(Deadline: 10am, 2022/11/11)

1. (30 points) Let (Gen, H) be a collision-resistant hash function. Is $(\mathsf{Gen}, \hat{H})$ defined by $\hat{H}^s(x) = H^s(H^s(x))$ necessarily collision resistant?

2. (20 points) Before HMAC, it was common to define a MAC for arbitrary-length messages by $\mathsf{Mac}_{s,k}(m) = H^s(k\|m)$ where H is a collision-resistant hash function. Show that this is never a secure MAC when H is constructed via the Merkle-Damgård transform. (Assume the hash key s is known to the attacker, and only k is kept secret.)