Foundations of Cryptography: Homework 11

(Deadline: Dec 13, 2018)

1. (20 points) Define a MAC for arbitrary-length messages by $\mathbf{Mac}((s,k),m) = H^s(k\|m)$ where $k \in \{0,1\}^n$ is an n-bit secret key and H is the collision-resistant hash function on page 2, lecture 21. Show that **Mac** is not EUF-CMA. (The s is public and known to the adversary. The k is secret and not known to the adversary.)

2. (10 points) Let p, q be two distinct primes. Show that $|\mathbb{Z}_{pq}^*| = (p-1)(q-1)$.