

## Cryptography ENEE/CMSC/MATH 456: Homework 5

Due by 2pm on 4/6/2020. Submission on Canvas.

1. Generalize the Merkle-Damgard construction for any compression function that compresses by at least one bit. You should refer to a general input length  $\ell'$  and general output length  $\ell$  (with  $\ell' > \ell$ ).
2. Consider defining a MAC by  $\text{Mac}_k(m) = H^s(k||m)$  where  $H$  is a collision-resistant hash function. Show that this is not a secure MAC when  $H$  is constructed via the Merkle-Damgard transform. As usual, assume that the hash key  $s$  is publicly known.
3. Assume collision-resistant hash functions exist. Show a construction of a fixed-length hash function  $(\text{Gen}, h)$  that is *not* collision resistant, but such that the hash function  $(\text{Gen}, H)$  obtained from the Merkle-Damgard transform to  $(\text{Gen}, h)$  is collision resistant.
4. Given a degree-5 LFSR with output sequence 1, 0, 0, 0, 0, 1, 0, 1, 1, 1 (where the output in time step 1 is on the left and the output in time step 10 is on the right). Determine the initial state and feedback coefficients of the LFSR.