Introduction to Cryptology ENEE459E/CMSC498R: Homework 6

Due by beginning of class on 3/31/2016.

1. Before HMAC was invented, it was quite common to define a MAC by $\mathsf{Mac}_k(m) = H^s(k||m)$ 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.

2. For each of the following modifications to the Merkle-Damgard transform, determine whether the result is collision resistant. If yes, provide a proof; if not, demonstrate an attack.

   Hint. For both parts below, if your answer is that it is insecure, you should design a specific compression function h which is collision-resistant, but for which the Merkle-Damgard transform is *not* collision resistant.

   (a) Modify the construction so that the input length is not included at all (i.e., output z_B and not $z_{B+1} = h^s(z_B||L)$). (Assume the resulting hash is only defined for inputs whose length is an integer multiple of the block length.)

   (b) Modify the construction so that instead of outputting $z = h^s(z_B||L)$, the algorithm outputs $z_B||L$.

3. Generalize the Merkle-Damgard construction for any compression function that compresses by at least one bit. You should refer to a general input length ℓ' and general output length ℓ (with $\ell' > \ell$).

4. Let $(\mathsf{Gen}; H)$ be a collision-resistant hash function and let F be a PRF. For each of the following, state whether $\widehat{H}$ is necessarily collision resistant. Justify your answer.

   (a) $\widehat{H}^s(x_1||x_2) := H^s(x_1)||H^s(x_2)$.

   (b) $\widehat{H}^s(x_1||x_2) := H^s(x_1 \oplus x_2)$.