CPSC 418/MATH 318 Practice Problems

Hash Functions and Message Authentication Codes

1. Let $H : \{0,1\}^* \to \{0,1\}^n$ be a (strongly) collision resistant hash function ($n > 0$). Define a hash function $H : \{0,1\}^* \to \{0,1\}^{n+1}$ as follows

$$H(x) = \begin{cases} 0\|x & \text{if } x \text{ has length } n, \\ 1\|h(x) & \text{otherwise,} \end{cases}$$

for all $x \in \{0,1\}^*$ where, as usual, "$\|$" denotes string concatenation.

   (a) Prove that H is not pre-image resistant.

   (b) Prove that H is (strongly) collision resistant.

2. Let $H_1, H_2 : \{0,1\}^* \to \{0,1\}^n$ be hash functions ($n > 0$). Define a hash function $H : \{0,1\}^* \to \{0,1\}^{2n}$ via $H(x) = H_1(x)\|H_2(x)$ for all $x \in \{0,1\}^*$.

   (a) Prove that H is collision resistant if at least one of H_1, H_2 is collision resistant.

   (b) Let H_1 be pre-image resistant and define $H_2 : \{0,1\}^* \to \{0,1\}^n$ via

$$H_2(x) = \begin{cases} \text{the last } n \text{ bits of } x & \text{if } x \text{ has length at least } n, \\ 0^{n-k}\|x & \text{if } x \text{ has length } k < n. \end{cases}$$

   Prove that H is not pre-image resistant for these choices of H_1, H_2.

3. Consider the following message authentication code called BCMAC (for "block cipher message authentication code") which is derived from a block cipher that operates on n-bit plaintexts. BCMAC takes as input a message M of bit length $2n-2$ and produces the corresponding tag as follows (here, E_K is encryption under the block cipher using key K and $\|$ denotes concatenation):

   (1) Write $M = M_0\|M_1$ where M_0, M_1 each have length $n-1$;
   (2) $\text{BCMAC}(M) = E_K(0\|M_0) \,\|\, E_K(1\|M_1)$.

   Show that BCMAC is not computation resistant.