CS 198 Codebreaking at Cal
Spring 2023 Makeup Assignment

Week 1

Question 1

Suppose we have a hash function H that takes in a bitstring M. We define $H(M) = M_1 \oplus M_2$, where we can split M in half as $M = M_1 || M_2$.

1. Is H preimage resistant?
2. Is H weak collision resistant?
3. Is H strong collision resistant?

Question 2

Instead of working with bitstrings, we decide to work with the set of English uppercase letters. Define $\alpha = \{A, B, \dots, Z\}$. Suppose we have a cryptographic hash function H that takes in variable-length messages and outputs a string of letters of length n (in math notation, $H : \alpha^* \to \alpha^n$).

Note: It's OK if your answer to either of the following 2 subparts is off by a constant factor (e.g. $\frac{1}{2}(2^n)$ instead of 2^n).

1. Suppose we know the hash $H(M)$ for an unknown message M. In terms of n, how many guesses do we need before the probability we've found M is over 50%?
2. In terms of n, how many messages M would we need to examine before the probability that we've found a collision (between any of the two messages we've looked at) is 50%?

Question 3

Suppose $Enc(K, M)$ is an IND-CPA secure encryption function that takes a key K and message M, and H is a cryptographic hash function. Alice and Bob share two symmetric keys K_1 and K_2 that Mallory doesn't know. Alice sends Bob $Enc(K_1, M)$ and $H(H(K_2 || M))$.

1. Does this scheme provide integrity? Why or why not?
2. Why is this scheme *not* IND-CPA secure?
3. Modify this scheme to make it IND-CPA secure.

Contributors:

- Ryan Cottone, Will Giorza