COMS 4995-001 (Science of Blockchains): Homework #5

Due by 11:59 PM on Wednesday, March 5th, 2025

Instructions:

(1) Solutions are to be completed and submitted in pairs.

(2) We are using Gradescope for homework submissions. See the course home page for instructions, the late day policy, and the School of Engineering honor code.

(3) Please type your solutions if possible and we encourage you to use the LaTeX template provided on the Courseworks page.

(4) Write convincingly but not excessively. (We reserve the right to deduct points for egregiously bad or excessive writing.)

(5) Except where otherwise noted, you may refer to your lecture notes and the specific supplementary readings listed on the course Web page *only*.

(6) You are not permitted to look up solutions to these problems on the Web. You should cite any outside sources that you used. All words should be your own. Submissions that violate these guidelines will (at best) be given zero credit, and may be treated as honor code violations.

(7) You can discuss the problems verbally at a high level with other pairs. And of course, you are encouraged to contact the course staff (via the discussion forum or office hours) for additional help.

(8) If you discuss solution approaches with anyone outside of your pair, you must list their names on the front page of your write-up.

Problem 1

(10 points) For this homework, you are tasked with carrying out a length-extension attack on SHA-256. For this question, we will be using an implementation of SHA-256/template code that we have uploaded to the course website. In more detail, your task is as follows.

1. We have chosen a 256-bit length private key k, which shall not be revealed. Consider now the function $f(z) = \text{SHA-256}(k||z)$, where "||" denotes concatenation. Let $x =$ "10010101". You are given that:

$$f(x) = 61fa41e8b85249da206e4101d5d52f2257aef2ad7139a096e1cb7f00a8734b43$$

where the right-hand side should be interpreted in hexadecimal. You are tasked with finding a (non empty) binary string y for which you can compute $f(x||y)$. For full credit, your provided string y must be *distinct* from all the solutions to this problem provided by the other students in the class (otherwise, only two-thirds credit will be awarded). In the template code provided, please insert your solution under the "YOUR CODE HERE" comment.