CSE 207B
Applied Cryptography

October 17, 2024
Due: October 29, 2024

Homework 4

Your homework should be submitted electronically via Gradescope before class on the due date. Please type up your solutions to the following problems using Latex and submit as `hw4-solutions.pdf`, along with text files containing the code you used to solve the first part as `hw4-sol.py`. Please credit any collaborators you worked with and any sources you used.

---

0. (a) Explain how you solved the decryption challenge.
   (b) *(optional)* This decryption challenge was completely new this year! Hopefully you found it fun. Were there any bugs you ran into, or any parts you found tedious/confusing/frustrating? Any suggestions for how we could improve this assignment in future years?

1. We want to build a collision-resistant hash function H using two collision-resistant hash functions H_1 and H_2, so that if at some future time one of H_1 or H_2 is broken (but not both) then H is still secure.

   (a) Suppose H_1 and H_2 are defined over (M, T). Let $H(m) := (H_1(m), H_2(m))$. Show that H is a secure collision-resistant hash function if either H_1 or H_2 is secure.

   (b) Show that $H'(x) := H_1(H_2(x))$ need not be a secure collision-resistant hash function even if one of H_1 or H_2 is secure — that is, if an adversary can *select* one of H_1 and H_2 to break (without finding a collision for the other), show they can use that to find a collision in $H'(x)$.

2. (Optional Extra Credit) If you came up with a second-preimage attack against MD2000: Turn in an additional file whose MD2000 hash equals the MD2000 hash of the string "`CSE 207B`" (but whose content is not the string "`CSE 207B`") and explain how you found it. Be warned we're not sure whether this is possible!