CSE 130 – INTRO TO CRYPTOGRAPHY

Spring 2025 Homework 3

Hash Functions and Applications:

1. (7 points) Consider the following modification to the Merkle-Damgård transform: append a 1 to the input x, followed by enough zeroes so that the length of the resulting string is n more than a multiple of n (i.e., $kn+n$ for some integer k). Parse the resulting string as $z_0, x_1, \ldots, x_B$, where $|z_0| = |x_i| = n$. Then for $i = 1, \ldots, B$, copute $z_i := h^s(z_{i-1}||x_i)$; output z_B.

   Show how to find a collision in the resulting hash function when this transform is applied to any compression function (Gen, h).

2. (10 points) Consider the following modification to the Merkle-Damgård transform: append a 1 to the input x, followed by enough zeroes so that the length of the resulting string is a multiple of n (i.e., kn for some integer k). Parse the resulting string as a sequence of n-bit blocks $x_1, \ldots, x_B$. Set $z_0 := 0^n$. Then for $i = 1, \ldots, B$, copute $z_i := h^s(z_{i-1}||x_i)$; output z_B.

   Assuming collision resistant compression functions exist, show that there exists a collision resistant compression function (Gen, h) such that this modified transform applied to (Gen, H) is not collision resistant. [Hint: Is it possible to efficiently find some $x_1 \in \{0,1\}^n$ such that $h^s(0^n, x_1) = 0^n$ for any s (assuming collision resistant compression functions exist)?]

3. (5 points) A student has 3,500 songs on her phone, and chooses songs to play at random. How many songs should the student expect to play before hearing some song twice (with probability at least 50%)?.

4. (10 points) Prove that the keyed function F given in Section 5.5.1 (pg. 179) is a pseudorandom function if H is modeled as a random oracle.

Practical Constructions of Symmetric-Key Primitives:

5. (5 points) Consider a degree-7 LFSR where only c_6, c_1, and c_0 are set to 1.

   (a) (3 points) What are the first 10 bits output by this LFSR if it starts in the initial state $(s_6, s_5, s_4, s_3, s_2, s_1, s_0) = (0, 0, 0, 0, 0, 0, 1)$?

   (b) (2 points) Show that this LFSR is not maximum length. [Hint: Find a nonzero state with a self-loop in the transition graph.]

6. (10 points) Consider a stream cipher constructed from two LFSRs A and B of degrees n_a and n_b, respectively, where the output at each clock tick is computed by taking the AND of the outputs of the two LFSRs. The key $k \in \{0,1\}^{n_a+n_b}$ is used to set the initial states of the two LFSRs.

   (a) (2 points) Show that this is never a secure stream cipher.

   (b) (8 points) Show that given a long enough output from this stream cipher, it is possible to recover the key in time $\approx 2^{n_a} + 2^{n_b}$.

7. (10 points) Fix a public, invertible permutation P, and define the keyed function $F_k(x) \stackrel{def}{=} P(\mathsf{const}||k||x)$. Show that F is not a pseudorandom function (describe the distinguisher and calculate the distinguishing probability).

8. (12 points) Let $\mathsf{Feistel}_{f_1,f_2}(\cdot)$ denote a two-round Feistel network using functions f_1 and f_2 (in that order). Define $\mathsf{swap}(L, R) = (R, L)$.

   (a) (6 points) Show that if

   $$(\hat{L}_2, \hat{R}_2) = \mathsf{swap}(\mathsf{Feistel}_{f_1,f_2}(L_0, R_0))$$

   then $(L_0, R_0) = \mathsf{swap}(\mathsf{Feistel}_{f_2,f_1}(\hat{L}_2, \hat{R}_2))$.

(b) (6 points) Show that if

$$(\hat{L}_{16}, \hat{R}_{16}) = \mathsf{swap}(\mathsf{Feistel}_{f_{15},f_{16}}(\cdots(\mathsf{Feistel}_{f_1,f_2}(L_0, R_0))\cdots))$$

then

$$(L_0, R_0) = \mathsf{swap}(\mathsf{Feistel}_{f_2,f_1}(\cdots(\mathsf{Feistel}_{f_{16},f_{15}}(\hat{L}_{16}, \hat{R}_{16}))\cdots))$$

Your submission must contain the following:

- Title that states "CSE 130 Homework 3 Solutions (Spring 2025)".
- Your full name (as it appears on CatCourses).
- The question number associated with each answer.
- Page numbers on each page. If submitting a handwritten scanned document (see below), your page numbers must be in the following format (1 of n, 2 of n, etc.), where n indicates the total number of pages.

The submission format is PDF. You may use the following to write your solutions:

- LaTeX: You may use the Overleaf online editor.
- Markdown: You may use VS Code for this (supports it natively). Please use the Print extension to save your rendered Markdown file as PDF.
- MS Word: You may use the built-in Equation Editor. Please make sure to save your Word file as PDF before submitting.
- Pen and Paper: Please make sure to scan your work as PDF before submitting (image formats like JPEG **will not be accepted**). Please make sure that your scanned document is **clearly legible** before submitting.