CSE 546
Cryptography **Homework 2** October 20, 2022

Important: The deadline for this homework is **3:00 pm on Monday 10/27/2022**. Late submissions *will not be accepted without a penalty.*

Instructions:

- This homework assignment is worth 100 points.
- While discussing problems with your classmates is allowed, your answers *must be in your own words.* Any exceptions will be punished, extending to reporting plagiarism according to departmental regulations. We know the online resources you would find for these problems, so use them at your own risk :)
- Be clear, succinct, and precise, but most importantly, be *rigorous.* Points not made are points lost.

Problem 1: CBC-based Encryption

Among the various modes of using block ciphers, we discussed the *chained-block cipher* or CBC method of encryption, and the related chained-CBC mode of encryption. This employed an uniformly chosen *initialization vector* IV at the beginning. We commented that it is crucial to the CPA security of this scheme that the IV is chosen uniformly.

(i) **(10 pts)** Show that the *chained-CBC* mode of encryption is not a CPA secure encryption scheme (described in the text in section 3.6.2, page 90, where you can recall its definition).

(ii) **(15 pts)** Consider yet another variant of CBC encryption called *incremental* CBC, where the encryption algorithm stores an IV, and increments it every time an encryption is performed. Show that this is also not CPA secure.

Problem 2: One-Way Functions

The following questions are about the notions of one-way functions and permutations.

(i) **(10 pts)** Let F be a (length-preserving) pseudorandom permutation. Prove that the function $f(x) = F_x(0^n)$ $(n = |x|)$ is one-way.

(ii) **(10 pts)** Let F be a (length-preserving) pseudorandom permutation. Prove that the function $f(x) = F_{0^n}(y)$ $(n = |y|)$ is not one-way.

Problem 3: More PRFs

A few more fun questions about PRFs! Let $F : \{0,1\}^n \times \{0,1\}^n \longrightarrow \{0,1\}^n$ be a (length-preserving) pseudorandom function.

(i) **(10 pts)** Let F' be the keyed function defined as $F'_k(x) = F_k(x)$ if x is even, and $F'_k(x) = F_k(x+1)$ if x is odd. State if F'_k is a PRF or not. If yes, provide a proof; if no, describe an attack.

(ii) **(15 pts)** Now consider the keyed function $F'' : \{0,1\}^n \times \{0,1\}^{n-1} \longrightarrow \{0,1\}^{2n}$ defined as

$$F''_k(x) = F_k(0||x)||F_k(1||x)$$

Prove that this is a PRF (by describing a reduction to the security of F).

Problem 4: Secure Hashing

Consider two hash functions (Gen_1, H_1) and (Gen_2, H_2). Consider a new hash function (Gen, H) defined as follows: Gen runs both Gen_1 and Gen_2 to obtain keys s_1 and s_2 respectively, and H is set to be $H^{s_1,s_2}(x) := H_1^{s_1}(x)||H_2^{s_2}(x)$. Prove or disprove:

(i) **(5 pts)** If H_1 and H_2 are both collision resistant, then H is also collision resistant.

(ii) **(10 pts)** If at least one of H_1 or H_2 is collision resistant, then H is collision resistant.

(iii) **(15 pts)** Finally, let $\tilde{H}^{s_1,s_2}(x) := H_1^{s_1}(H_2^{s_2}(x))$. Prove or disprove that if both are H_1 and H_2 are collision resistant, then $\tilde{H}$ is collision resistant.