Homework 6

Due: November 3, 2023

CS 1510: Intro. to Cryptography and Computer Security

1 Block Cipher Modes of Operation

In this problem, we will explore the differences in errors between the CBC, OFB, and CTR modes of operation.

a. Consider the case in which there is a single-bit error in the ciphertext. What is the effect on the output of the CBC, OFB, and CTR modes of operation?

b. Consider the case in which there is a dropped ciphertext block (in other words, if the transmitted ciphertext $c_0, c_1, c_2, c_3, \ldots$ is received as $c_0, c_1, c_3, \ldots$). What is the effect on the output of the CBC, OFB, and CTR modes of operation?

2 Hardcore Predicates for One-Way Functions

Let f be a one-way function. Define a function $B : \{0,1\}^* \to \{0,1\}$ for f, where $B(x)$ outputs the inner product modulo 2 of the first $\lfloor |x|/2 \rfloor$ bits of x and the last $\lfloor |x|/2 \rfloor$ bits of x. Prove or disprove that B is a hard-core predicate for f.

3 One-Way Functions

Let $|x|$ denote the length of the binary string x, let $\|$ denote the concatenation operator, and let $(\|)$ denote the parse operator such that when we parse $x = x_1(\|)x_2$, we get $|x_1| = |x_2|$. (Assume for simplicity that all strings to which the parse operator is applied are of even length; this can be accomplished, for example, by appending a 0 to the end of an odd-length string prior to applying the parse operator.) Suppose that $g(x)$ is a one-way function that is length-preserving, meaning that $|g(x)| = |x|$ and also that we need not give the adversary 1^k as input.

For the following functions, use a reduction to prove that the function is one-way, or give a counterexample showing that it is not one-way.

a. $f_a(x) = g(x) \oplus x$.

b. $f_b(x) = g(x_1 \oplus x_2)$, where $x = x_1(\|)x_2$.

c. $f_c(x) = \begin{cases} 0^{|x|} & \text{if exactly 1 bit of } x_1 \text{ is 1,} \\ 0^{|x_1|} \| g(x_2) & \text{otherwise} \end{cases}$ where $x = x_1(\|)x_2$.

d. $f_d(x) = \begin{cases} 0^{|x|} & \text{if at least 1 bit of } x_1 \text{ is 1,} \\ 0^{|x_1|} \| g(x_2) & \text{otherwise} \end{cases}$ where $x = x_1(\|)x_2$.

4 One-Way Functions Imply that $P \neq NP$

Prove that the existence of one-way functions implies $P \neq NP$.

5 Summary Question

Summarize the most important insights from this week's material, including from the lectures, notes, textbooks, homework problems, and other resources you find helpful, into a one-page resource. You will be permitted to use this one-page resource (along with the other weeks' resources) on the midterm and final.

Changes to this document prior to the exams are permitted, but for each change, you will be asked to state what you changed and why. For example, if you dropped something and replaced it with something else, justify why the thing you dropped wasn't as important as the thing you inserted, why you think it might be more useful for the exam, etc.

Please note that the purpose of this question is to help you organize and synthesize the material for your own future use. It will be graded based on completion—we will not be checking it for correctness.