Problem Set #4

CMSC/Math 456
Instructor: Daniel Gottesman

Due on Gradscope, Thursday, Sep. 28, noon (before start of class)

General instructions: If you collaborate or use any outside resources, remember to cite them in your solutions.

Note: This problem set has 3 problems; problem 3 is on page 2.

Problem #1. Pseudorandom Functions (40 points)

For this problem, assume $F_k(x)$ is a pseudorandom function that takes n-bit inputs and gives n-bit outputs. You may also assume that k is n bits long.

As the answer to each of these problems, give a range of possible values of probability which could possibly be achieved by different families of functions satisfying the definition of security for pseudorandom functions. Narrow down the probability to the smallest range you can. You may use big-O notation and/or negligible functions to define the range.

For instance, you might say that the probability is between 0 and $O(1/n)$. This would be an acceptable answer if the correct range is between 0 and $2/n$, but inadequate if the correct range is between 0 and $2/n^2$, since then you could have a narrower range.

a) (15 points) What can you say about the probability, for uniformly random x and k, that the first bit of $F_k(x)$ is 1? Justify your answer.

b) (15 points) What can you say about the probability, for uniformly random x, y, and k, that $F_k(x) = F_k(y)$? Justify your answer.

c) (10 points) What can you say about the probability, for uniformly random k, that $F_k(x) \neq F_k(y)$ for *all* x and y? Justify your answer.

Problem #2. CPA security (40 points)

a) (20 points) Let $G_1(k)$ and $G_2(k)$ be pseudorandom generators with output length n and let k be a secret key string. Consider the following encryption protocol: Generate random string IV of length n. Given a message $m = (m_A, m_B)$ in two blocks each of length n, let the ciphertext be (IV, c_A, c_B), with

$$\begin{aligned} c_A &= m_A \oplus G_1(k) \oplus IV \\ c_B &= m_B \oplus G_2(k) \oplus c_A. \end{aligned} \tag{1}$$

Find an attack that shows that this protocol is not CPA secure.

b) (20 points) Let $F_k(x)$ be a pseudorandom function with input and output length n and let k be a secret key string. Consider the following encryption protocol: Generate random string IV of length n. Given a message $m = (m_A, m_B)$ in two blocks each of length n, let the ciphertext be (IV, c_A, c_B), with

$$\begin{aligned} c_A &= m_A \oplus F_k(IV) \\ c_B &= m_B \oplus F_k(m_A). \end{aligned} \tag{2}$$

Find an attack that shows that this protocol is not CPA secure.

Problem #3. Substitution Permutation Networks (40 points)

In this problem, consider a substitution permutation network composed of $8n$ bits, with $n = 2^s$, s a positive integer. The bits are labelled by a pair (j, k), with j a number from 0 to 7 and k an s-bit binary number $k_0k_1k_2 \ldots k_{s-1}$. That is, k_0 is the most significant bit of k and k_{s-1} is the least significant bit, so for instance, if $k = 4$, its binary representation is 100 and $k_0 = 1$, $k_1 = 0$, and $k_2 = 0$.

In the substitution permutation network, the bits are mixed with a key via XOR, then divided up into groups of 8 and passed through S-boxes. Bits with the same k label go into the same S-box. The S-boxes take 8-bit inputs and produce 8-bit outputs.

Then the bits are passed to one of the following transformations, which relabel bit (j, k) as bit (j', k') (for all (j, k)), completing one round. The same sequence of steps is repeated for many rounds.

Only one of the transformations below is a possible candidate to produce a substitution permutation network with an avalanche effect. Identify which one and for each of the candidates, describe your reasoning for why it is or is not the correct choice. (10 points for each candidate.)

a) $(j, k) \to (j', k')$ with $k' = k$ for all k, $j' = j + 1$ if j is even, and $j' = j - 1$ if j is odd.

b) $(j, k) \to (j', k')$ with $j' = j + 4 \bmod 8$, $k'_i = 1 \oplus k'_i$ for i odd, and $k'_i = k_i$ for i even. (That is, the odd numbered bits of k are flipped.)

c) $(j, k) \to (j', k')$ with $j' = 3j \bmod 8$ and $k' = (3k + j) \bmod n$.

d) $(j, k) \to (j', k')$ with $j' = 4j \bmod 8$ and $k' = (4k + j) \bmod n$.