Homework 4 - CSCI 181

5 questions 40 points

1. (10 points) Suppose we have a hash function h that takes inputs of 1088 bit strings and outputs hash strings of 256 bits.

   (a) As discussed this function will have collisions, and on average, h is an n-to-1 map. Find n.

   (b) For an output y, we expect to have n input strings that map to it. So there will be n different 1088 bit strings x such that $h(x) = y$. If we want to solve the one-way problem for an output string y, we need to find one of the n x's among all 1088 bit strings. This seems easy to do as we only need to find ANY 1088 bit string x such that $h(x) = y$ and we have n of such x's. However, the probability that we will solve the one-way problem by applying h to random 1088 bit strings is n/(number of 1088 bit strings). Find this probability for this hash function.

2. (10 points) Let $f : X \to Y$ be a hash function and assume $|X|/|Y|$ is very large (note $|X|$ and $|Y|$ are the sizes of the sets X and Y, respectively). Write an informal proof that if f has the weakly collision resistant property then f has the one-way property. You can do this by writing a contrapositive proof. So assume that f does NOT have the one-way property, and then give an informal proof that f will NOT have the the weakly collision resistant property.

   Recall: One-way property: Given $y \in Y$ it is infeasible to find $x \in X$ such that $f(x) = y$.

   Weakly collision resistant property: Given $x \in X$ it is infeasible to find $x' \in X$ with $x' \neq x$ such that $f(x') = f(x)$.

For the next questions: Implement the following functions all in one program file. A file called sha3in.txt is provided to you which is a file of 1600 bits. This is the input to your program. Read in this file into your program and answer the questions based on this input file.

3. (5 points) Implement a function called inputSHA3() that turns a 1-dimensional array of length 1600, $v[0 \ldots 1599]$, to a 3-dimensional array $a[0 \ldots 4][0 \ldots 4][0 \ldots 63]$ such that $a[i][j][k] = v[64(5j + i) + k]$.

4. (5 points) Implement a function called outputSHA3() that turns a 3-dimensional array $a[0 \ldots 4][0 \ldots 4][0 \ldots 63]$ into a 1-dimensional array of length 1600, $v[0 \ldots 1599]$, such that $v[64(5j + i) + k] = a[i][j][k]$.

5. (10 points) Implement the function θ from a 3-dimensional array $a_{in}[0 \ldots 4][0 \ldots 4][0 \ldots 63]$ to a 3-dimensional array $a_{out}[0 \ldots 4][0 \ldots 4][0 \ldots 63]$. To check your work, apply your function to the input file provided and the output $a_{out}[4][3][9 \ldots 18]$ should be 0011011000. Apply θ to the input file provided. In your homework writeup, list the ten bits

$a_{out}[3][1][15 \ldots 24]$.

Homework 4 ends here. If you want to get a head start on next week's assignment you can start implementing the next functions. But please do not submit them at this time. You will see these questions again as part of the next homework.

NextQuestion. Implement the function ρ from a 3-dimensional array $a_{in}[0 \ldots 4][0 \ldots 4][0 \ldots 63]$ to a 3-dimensional array $a_{out}[0 \ldots 4][0 \ldots 4][0 \ldots 63]$. Note that the rho matrix is:

rhomatrix=[0,36,3,41,18;1,44,10,45,2;62,6,43,15,61;28,55,25,21,56;27,20,39,8,14]

To check your work, apply your function to the input file provided to you, the output $a_{out}[4][3][9 \ldots 18]$ should be 0110011001.

Apply ρ to the input file provided. In your homework writeup, list the ten bits $a_{out}[3][1][15 \ldots 24]$.

NextQuestion. Implement the function π from a 3-dimensional array $a_{in}[0 \ldots 4][0 \ldots 4][0 \ldots 63]$ to a 3-dimensional array $a_{out}[0 \ldots 4][0 \ldots 4][0 \ldots 63]$. To check your work, apply your function to the input file provided and the output $a_{out}[4][3][9 \ldots 18]$ should be 0110110001. Apply π to the input file provided. In your homework writeup, list the ten bits $a_{out}[3][1][15 \ldots 24]$.