Homework 5 - CSCI 181 - S20

Implement the following functions all in one program. 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.

1. (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 $a[i][j][k] = v[64(5j + i) + k]$.

2. (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 $v[64(5j + i) + k] = a[i][j][k]$.

3. (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 $a_{out}[2][3][11 \ldots 20]$.

4. (10 points) 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 in the file, 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 $a_{out}[2][3][11 \ldots 20]$.

5. (10 points) 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 to the input file provided. In your homework writeup, list the ten bits $a_{out}[2][3][11 \ldots 20]$.