Homework 5 - CSCI 181

1. (15 points) As mentioned in the lecture, in a hash function the word diffusion refers to how the change of a single bit in input can affect many different bits in the output. Consider a single application of θ step.

   (a) If we change the bit in $a_{in}[1][4][63]$ which bits exactly are affected in a_{out}? Remember that *affected* does not necessarily mean the bit changed, it means that there is the potential for change.

   (b) How many unique bits will be affected if you apply the θ step for a second round? (Note that we are assuming that we are only applying θ and not any of the other functions.) Show which bits are affected.

2. (10 points) Find RC[3] in the iota step. Write RC[3] in hex similar to RC[0] and RC[1] that is provided in the lecture. Show your work by checking the constant term of x^t similar to the approach in the lecture.

3. (10 points) [Programming assignment] Implement the function ρ from a 3-dimensional array $a_{in}[0\dots4][0\dots4][0\dots63]$ to a 3-dimensional array $a_{out}[0\dots4][0\dots4][0\dots63]$. 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 $a_{out}[4][3][9\dots18]$ should be 0110011001.

   Apply ρ to the input file provided. In your homework writeup, list the ten bits $a_{out}[3][1][15\dots24]$.

4. (10 points) [Programming assignment] Implement the function π from a 3-dimensional array $a_{in}[0\dots4][0\dots4][0\dots63]$ to a 3-dimensional array $a_{out}[0\dots4][0\dots4][0\dots63]$. To check your work, apply your function to the input file provided and the output $a_{out}[4][3][9\dots18]$ should be 0110110001. Apply π to the input file provided. In your homework writeup, list the ten bits $a_{out}[3][1][15\dots24]$.

5. (10 points) [Programming assignment] Implement the function χ from a 3-dimensional array $a_{in}[0\dots4][0\dots4][0\dots63]$ to a 3-dimensional array $a_{out}[0\dots4][0\dots4][0\dots63]$.

   To check your work, apply your function to the input file provided (sha3in.txt) and the output $a_{out}[4][3][9\dots18]$ should be 0110100001. Apply χ to the input file provided. In your homework writeup, write down the ten bits $a_{out}[3][1][15\dots24]$.