Homework 6 - part 1- CSCI 181 - S20

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 $a_{in}[2][1][24]$ 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 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.)

2. (10 points) Find RC[2] in the iota step. Write RC[2] 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.