

### **Fall 2019 CIS 3362 Homework #4 Grading Criteria**

Question 1: 8 pts (1/2 pt per entry round down, if you see an incorrect cohesive system, feel free to give 4 of 8)

Question 2: 8 pts (1/2 pt per entry round down, if you see an incorrect cohesive system, feel free to give 4 of 8)

Question 3: 18 pts (2 pts per s-box, give partial as needed, 2 pts to convert to hex in the end.)

Question 4: 12 pts (1 pt per hex char)

Question 5: 10 pts (4 pts for key space calculation, 2 pts to get #3 of seconds, 4 pts to convert to hours, min and sec)

Question 6: 16 pts (4 pts for the correct sum of products, 2 pts for keeping both 1 times the same, 4 pts for the 2 times, 4 pts for the 3 times, 2 pts for final XOR)

Question 7: 8 pts (1 pt per hex char in XOR)

Question 8: 12 pts (1 pt rotate, 4 pts sub word, 1 pt rcon, 2 pts xor, 4 pts final result)

Question 9: 10 pts (Give full credit to any valid explanation, decide partial as you see fit.)

Question 10: 20 pts (10 pts for grabbing the appropriate code from AES.java, 10 pts for the double for loop - please make sure to match their output to both files I've included, multtable.out and multtable\_old.out. My guess is that most will match the latter and will not have error corrected my mistake.) Give partial as you see fit if you see little issues with the code like forgetting the newline, or something of that nature.