Fall 2020 CIS 3362 Quiz #3 Part A: DES

Date: 10/12/2020

Directions: Please use DES/AES and Binary->Hex reference sheets, your course notes and a calculator as aids for this exam. Do NOT attempt to look up information online. Even if you use a calculator, show each step of your calculations that you would do by hand. The role of the calculator will simply be to speed up individual calculations (13 x 29, for example), not to skip whole steps, as these steps are typically awarded points in the grading criteria.

Please either type your answers. The accepted file types for submission will be .doc, .docx, .txt and .pdf. I recommend that you directly type into the posted document to save time.

Please look at Webcourses to see when your due time and late due time are. It's recommended that you stop working at the due time and start uploading at that time. Anything turned in before the late due time will be accepted for full credit. Anything that doesn't make it in by the late due time will earn a 0. A 10 minute buffer will be provided after both due times. Please don't take advantage of these buffers as it's an unnecessary risk.

1) (9 pts) Let S_k represent applying the k^{th} S-box in DES. The input for S_k is 6 bits. Show the output, **in binary**, for the three following S-box look ups:

a) $S_3(010111)$ b) $S_6(101110)$ c) $S_7(001000)$

For each answer, please clearly indicate which row and which column you have found the appropriate entry, and then also convert it to binary.

2) (8 pts) Let the plaintext for a DES block (in hex) be 7e 9f 3c 62 1a 80 5b 4d. Give the first eight bits of the transformed input after applying the IP matrix. In order to get credit, show your work clearly (indicate WHICH bits you are grabbing.) No credit will be given for the correct answers since randomly guessing will get half the credit. Rather, all the credit will be given for showing the process to use.

3) (8 pts) Consider doing a brute force search on a DES key when the even key bits, k_2, k_4, k_6, …, k_{64} are known and you can test 2^{20} keys per second. (Note: the bit representation is the one given in the official documentation where the key is given with parity bits.) How long will it take to finish the search in hours, minutes and seconds?