## CIS 3362 Test #2: Modern Symmetric Encryption Schemes (DES, AES) Date: 10/26/2016

		 		10022200	 		 	_	
 .: dam a 16 h	4 1 - 1 1 -	 414	~ ~		 	1)	 41	~ ~ ~	+

First Name:

1) (8 pts) Consider a 16 bit block cipher that uses a permutation matrix, P', in the same format as IP in DES, given below. Let the 16 bit plaintext input to the matrix P' be 1001 0111 1011 0011. What is the output? (Express your answer as 16 bits.)

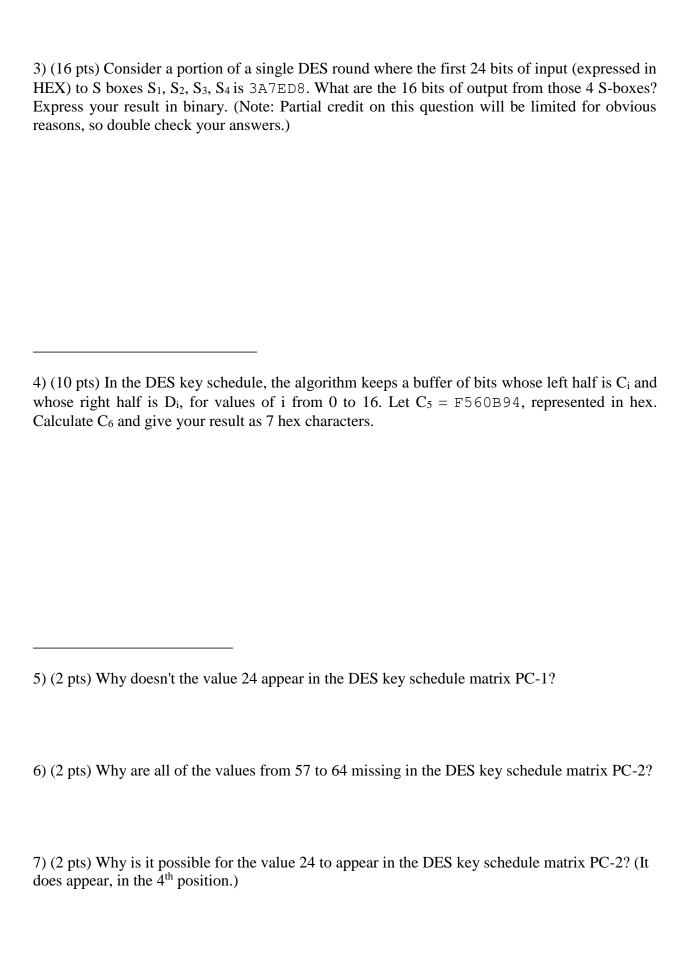
$$\begin{bmatrix} 14 & 10 & 3 & 7 \\ 9 & 12 & 13 & 15 \\ 6 & 11 & 8 & 4 \\ 16 & 2 & 5 & 1 \end{bmatrix}$$

2) (12 pts) You are attempting to brute force a DES key. Luckily, you have obtained the following bit locations of the key (out of the locations  $k_1$ ,  $k_2$ , ...  $k_{64}$  given in the official specification):

 $k_1$ ,  $k_5$ ,  $k_8$ ,  $k_{17}$ ,  $k_{18}$ ,  $k_{19}$ ,  $k_{20}$ ,  $k_{21}$ ,  $k_{22}$ ,  $k_{23}$ ,  $k_{24}$ ,  $k_{42}$ ,  $k_{44}$ ,  $k_{45}$ ,  $k_{47}$ ,  $k_{56}$ ,  $k_{60}$ , and  $k_{64}$ 

Last Name:

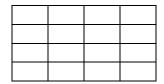
How many keys do you have to try to ensure that you find the appropriate key? (Assume that we have a matching plaintext and ciphertext block we can use to verify if a guess to the key is correct or not and the correct bits for the bit locations specified above in the key.) Please leave your answer as a power of 2.



8) (8 pts) Let the state matrix to AES right before the SubBytes step be the matrix shown below. Show the state of the matrix right AFTER the SubBytes step:

3D	FF	09	31		
85	4B	75	E2		
С6	BD	2E	18		
5A	6C	Α0	E4		

9) (8 pts) Let the state matrix to AES right before the ShiftRows step be your answer from problem 8. Show the state of the matrix right AFTER the ShiftRows step:



10) (12 pts) Consider the process of AES Key Expansion. Imagine that we have:

w[16] = 54 9E B6 38 (in hex) w[19] = 01 F7 AD C2 (in hex)

Calculate w[20], showing each of the following intermediate results: RotWord(temp), SubWord(RotWord(temp)), Rcon[i/4], and the result of the XOR with Rcon[i/4].

RotWord	SubWord	Rcon[i/4]	XOR	FinalResult	



Scratch Page - Please clearly mark any work on this page you would like graded.