CIS 3362 Quiz #3: Bitwise Operators, DES, AES

Date: 10/6/2025

Name : _____

1) (8 pts) Consider a DES-like cipher that operates on 16 bit blocks with the following IP matrix:

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

Consider defining a new matrix NP which is the result of applying IP twice. (So for example, the original bit in position 1 goes to position 15 when IP is applied once. Then, when we apply IP a second time, that bit goes from position 15 to position 3. Thus, NP[1][3], using 1-based indexing would equal 1, since for NP, we would want to place the original bit in position 1 into position 3 after the application of NP. Please fill in the blanks below.

___ ___ ___ ___

___ ___ ___ ___

___ ___ ___ ___

___ ___ ___ ___

2) (8 pts) Provide the output for the designated inputs for each of the four S-boxes described below. Please give your answers as **4 binary bits.** (Each answer is worth 2 pts, no partial credit, so carefully make sure you are **using the correct S-box** and look up the correct row and column. **Half credit is given to correct decimal or hex answers.**)

(a) $S_3(011011)$ = _____

(b) $S_5(101101)$ = _____

(c) $S_6(110000)$ = _____

(d) $S_7(010110)$ = _____

3) (10 pts) Consider the task of writing a function (**in C**) that takes in a single unsigned long long storing a potential DES key with parity bits, with the most significant bit storing k_1 (first bit of key) and the least significant bit storing k_{64}, a parity bit, that determines if the parity bits are valid or not. Complete the function below so that it returns 1 if all 8 parity bits are valid, and 0 otherwise. (Note: The code isn't that long but I am just providing the space anyway...) Note: If you want to left shift the value of 1 in a unsigned long long, please write **`1llu`**.

```
int isValidDESKey(unsigned long long key) {




}
```

4) (4 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:

31	9A	5C	B5
A6	27	4E	F0
15	6F	C2	8D
D4	73	08	EC

5) (8 pts) Consider the process of AES Key Expansion. Imagine that we have:

w[20] = D4 69 C2 0A (in hex)
w[23] = 1B 37 E5 8F (in hex)

Calculate w[24] and express your answer as **8 HEX characters.** (Show your answer after each step designated below:

temp = _____

After RotWord = _____

After SubWord = _____

Rcon(___) = _____

After XOR w/Rcon = _____

w[____] = _____

Final Answer = _____

6) (10 pts) Let the state matrix to AES right before the MixCols step be the matrix shown below. What is the value of the entry in **row 1, column 3 (1-based indexing).** right AFTER the MixCols step? Express your answer as **2 HEX characters.** **(Note:** Automatic 0 out of 10 if your sum of products is for the wrong entry.**)**

32	97	93	19
A4	AC	E5	E3
B9	3B	4F	46
47	D6	C7	6F

___ ___

7) (1 pt) University of Wisconsin's mascot is Bucky the Badger. After which animal is the University of Wisconsin's mascot based?

_____

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