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

Date: 10/6/2025

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.

15	**16**	**1**	**6**
8	**14**	**11**	**13**
12	**9**	**4**	**2**
5	**7**	**3**	**10**

Grading: 1/2 pt per entry round down, no exceptions

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) $S_3(011011)$ = **1011** row = 01 = 1, col = 1101 = 13, $S_3[1][13]$ = 11 in binary 1011

(b) $S_5(101101)$ = **0010** row = 11 = 3, col = 0110 = 6, $S_5[3][6]$ = 2 in binary 0010

(c) $S_6(110000)$ = **0111** row = 10 = 2, col = 1000 = 8, $S_6[2][8]$ = 7 in binary 0111

(d) $S_7(010110)$ = **0111** row = 00 = 0, col = 1011 = 11, $S_7[0][11]$ = 7 in binary 0111

Grading: 1 pt for correct decimal answer, 2 pts for correct binary answer, 0 otherwise.

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...)

Two possible solutions are shown below:

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

    for (int i=0; i<8; i++) {

        int odd = 0;
        unsigned long long tmp = key & 255;

        for (int j=0; j<8; j++)
            if (tmp&(1<<j))
                odd^=1;

        if (!odd) return 0;

        key >>= 8;
    }

    return 1;
}
```

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

    for (int i=0; i<8; i++) {

        int odd = 0;
        for (int j=0; j<8; j++)
            if (key&(1llu<<(8*i+j)))
                odd^=1;

        if (!odd) return 0;
    }

    return 1;
}
```

Grading:

Looping through each byte one which way or the other – 2 pts
Only returning 1 at the very end after all bytes checked – 2 pts
Trying to check each byte and returning 0 inside outer loop if it doesn't "pass" (even if their test is wrong) – 2 pts
Validity of checking a byte – 4 pts
(Grader decides partial for this past part.)

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

C7	B8	4A	D5
24	CC	2F	8C
59	A8	25	5D
48	8F	30	CE

Grading: 1/4 pt each, record grade as floor(score out of 4).

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 = **1B 37 E5 8F** **Grading: 1 pt**

After RotWord = **37 E5 8F 1B** **Grading: 1 pt**

After SubWord = **9A D9 73 AF** **Grading: 1 pt**

Rcon(**6**) = **20 00 00 00** **Grading: 1 pt**

After XOR w/Rcon = **BA D9 73 AF** **Grading: 1 pt**

w[**20**] = **D4 69 C2 0A** **Grading: 1 pt**

Final Answer = **6E B0 B1 A5** **Grading: 2 pts**

Note: Grader may give carry over credit for an early wrong step, but isn't required to do so.

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

Row 1, Col 3 =02 x 93 + 03 x E5 + 01 x 4F + 01 x C7

02 x 93 = 1001 0011 0 = 0010 0110
+ 1 1011

0011 1101 (3D)

03 x E5 = 02 x E5 + 01 x E5

02 x E5 = 1110 0101 0 = 1100 1010
+ 1 1011

1101 0001

03 x E5 = 02 x E5 = 1101 0001
+ 01 x E5 = 1110 0101

0011 0100 (34)

Final Answer = 3D + 34 + 4F + C7 = **81**

Grading: auto 0 of wrong entry is listed
2 pts for listing correct sum of products
2 pts for 02 x 93
4 pts for 03 x E5
2 pts for final XOR (if answer is in binary give 1 of these 2 pts if correct)

7) (2 pts) University of Wisconsin's mascot is Bucky the Badger. After which animal is the University of Wisconsin's mascot based?

Badger (Grading: Give to All)