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

1) (5 pts) Explain, in words, what value this function returns in terms of its input value, x. Please explain in plain English. Any "literal translation" (things like, "this bit gets shifted and then, etc.") will get **NO credit.** (Note: The space I have provided is limited because I am looking for a single sentence answer.)

```
int whatdoesitdo(int x) {
    int y = 0;
    while (x > 0) {
        y = (y << 1);
        y = (y | (x & 1));
        x = (x >> 1);
    }
    return y;
}
```

Solution

It returns the value that is the reverse binary representation of x.

Grading: 2 pts for anything mentioning binary representation, 3 pts for mentioning reverse.

2) (6 pts) Let the input to the DES encryption algorithm, in HEX, for a 64 bit block be

8E4F 97CA 4607 BE15

After applying IP to this input, what are the first 24 bits of output? Please express your answer as **6 HEX characters.**

Solution

Write out the bits in an 8 by 8 format so it's easy to grab the bits we want:

1000 1110
0100 1111
1001 0111
1100 1010
0100 0110
0000 0111
1011 1110
0001 0101

Now, using IP, we grab the bits designated: 58th bit, 50th bit, etc. until we take the 6th bit. I've highlighted the bits taken in yellow (first 8), green (next 8) and purple (third 8).

Bits are: 0001 1010 1100 0100 1111 0111, converted to HEX we have: **1AC4F7. Grading: 1 pt per hex char, all or nothing on each.**

3) (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.)

Solution

(a) $S_3(101110)$ = **0000,** row = $10_2 = 2$, col = $0111_2 = 7$

(b) $S_4(010111)$ = **1100,** row = $01_2 = 1$, col = $1011_2 = B$

(c) $S_6(100101)$ = **0010,** row = $11_2 = 3$, col = $0010_2 = 2$

(d) $S_7(011010)$ = **1010,** row = $00_2 = 0$, col = $1101_2 = D$

Grading: 2 pts for each answer in binary, 1 pt if the correct answer is in base ten or hex, 0 pts otherwise

4) (8 pts) Consider the DES Key Schedule algorithm. Imagine that in the middle of the algorithm, we have the following values for C_2 and D_2, in binary:

```
C2 = 1011 0000 1010 0111 1101 0101 1100
D2 = 0001 0110 1100 1010 1111 1001 0011
```

Please show your work and determine the first 16 bits of K_3, the round 3 key. (Note: since random luck will get 8 bits correct, the scoring on this question will simply be max(0, correctbits-8).)

Solution

First, do a left shift of 2 bits (round 3 is 2 bits rotated) on both buffers:

```
C2 = 11 0000 1010 0111 1101 0101 1100 10
D2 = 01 0110 1100 1010 1111 1001 0011 00
```

Then, we will use PC-2 to select the bit locations 14, 17, 11, 24, 1, 5, 3, 28, 15, 6, 21, 10, 23, 19, 12, 4. The selected bits are highlighted and the result is shown below:

1001 1000 1000 1010

Grading: 0 pts if there are 8 or fewer correct bits, x -8 pts otherwise, where x is the correct number of bits.

5) (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:

32	16	8D	19
A4	8F	5E	E3
B9	92	21	46
47	CA	D7	6F

23	47	5D	D4
49	73	58	11
56	4F	FD	5A
A0	74	0E	A8

Grading: 1/2 each, round down

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 2, column 1, right AFTER the MixCols step? Express your answer as **2 HEX characters.**

32	16	8D	19
A4	8F	5E	E3
B9	92	21	46
47	CA	D7	6F

Solution

We desire the value of 01x32 + 02xA4 + 03xB9 + 01x47.

Here is the work for the two middle terms:

```
02 x A4 = 1010 0100 0 =
           0100 1000
         +   1 1011
         ----------
          0101 0011 (53)
```

```
03 x B9 = 02 x B9 + 01 x B9
01 x B9 = 1011 1001 (B9)
02 x B9 = 1011 1001 0 =
           0111 0010
         +   1 1011
         ----------
          0110 1001 (69)
03 x B9 = B9 + 69 = D0
```

Final answer is 32 + 53 + D0 + 47 = 61 + 97 = **F6**

Grading: 1 pt each mult by 1, 2 pts mult by 2, 3 pts mult by 3, 3 pts final XOR

7) (4 pts) Consider the process of AES Key Expansion. Imagine that we have:

w[22] = 01 32 45 76 (in hex)
w[25] = 89 BA CD FE (in hex)

Calculate w[26] and express your answer as **8 HEXcharacters.**

Solution
Since 26 ≡ 2 (mod 4), we simply XOR the two words shown above to get:

```
w[26] = 88 88 88 88
```

Grading: 1 pt per byte, must have the byte correct to get the point.

8) (1 pt) By what acronym is the National Security Agency better known? **NSA (Give to All)**