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.)

```c
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:

```
100 1110
010 1111
100 0111
110 1010
010 0110
000 0111
101 1110
000 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) \( S_3(101110) = \underbrace{0000}, \) row = 102 = 2, col = 01112 = 7
(b) \( S_4(010111) = \underbrace{1100}, \) row = 012 = 1, col = 10112 = B
(c) \( S_6(100101) = \underbrace{0010}, \) row = 112 = 3, col = 00102 = 2
(d) \( S_7(011010) = \underbrace{1010}, \) row = 002 = 0, col = 11012 = 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:

\[
\begin{align*}
C_2 &= 1011 0000 1010 0111 1101 0101 1100 \\
D_2 &= 0001 0110 1100 1010 1111 1001 0011
\end{align*}
\]

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 \( \max(0, \text{correctbits}-8) \).)

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

\[
\begin{align*}
C_2 &= \underbrace{11 0000 1010 0111 1101 0101 1100} \\
D_2 &= \underbrace{01 0110 1100 1010 1111 1001 0011 00}
\end{align*}
\]

Then, we will use \( \text{PC}-2 \) 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:

\[
\underbrace{1001 1000 1000 1010}
\]

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:

<table>
<thead>
<tr>
<th>32</th>
<th>16</th>
<th>8D</th>
<th>19</th>
</tr>
</thead>
<tbody>
<tr>
<td>A4</td>
<td>8F</td>
<td>5E</td>
<td>E3</td>
</tr>
<tr>
<td>B9</td>
<td>92</td>
<td>21</td>
<td>46</td>
</tr>
<tr>
<td>47</td>
<td>CA</td>
<td>D7</td>
<td>6F</td>
</tr>
</tbody>
</table>

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.

<table>
<thead>
<tr>
<th>32</th>
<th>16</th>
<th>8D</th>
<th>19</th>
</tr>
</thead>
<tbody>
<tr>
<td>A4</td>
<td>8F</td>
<td>5E</td>
<td>E3</td>
</tr>
<tr>
<td>B9</td>
<td>92</td>
<td>21</td>
<td>46</td>
</tr>
<tr>
<td>47</td>
<td>CA</td>
<td>D7</td>
<td>6F</td>
</tr>
</tbody>
</table>

**Solution**
We desire the value of $01 \times 32 + 02 \times A4 + 03 \times B9 + 01 \times 47$.

Here is the work for the two middle terms:

$02 \times A4 = 1010 0100 0 = 03 \times B9 = 02 \times B9 + 01 \times B9$

$0100 1000$

$+ 1 1011$

----------

$0101 0011 (53)$

$03 \times B9 = B9 + 69 = D0$

Final answer is $32 + 53 + D0 + 47 = 61 + 97 = \textbf{F6}$

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:

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

Calculate \( w[26] \) and express your answer as 8 \text{ HEXcharacters}.

\textbf{Solution}

Since \( 26 \equiv 2 \pmod{4} \), we simply XOR the two words shown above to get:

\[ w[26] = 88 \ 88 \ 88 \ 88 \]

\textbf{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? \textbf{NSA (Give to All)}