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

Date: 10/9/2023

1) (5 pts) What is the output of the following program?

```
int main() {
    int x = (1<<21) + (1<<17) + (1<<13) + (1<<9) + (1<<7) + (1<<1);
    int mask = (1<<8)-1;
    int res = 0;
    for (int i=0; i<3; i++) {
        res = res ^ (mask&x);
        x = (x>>8);
    }
    printf("%d\n", res);
    return 0;
}
```

The code separates x into its three least significant bytes and XORs these bytes together. The variable mask is set to 8 1's in binary, so if you and with this mask, you're isolating the least significant byte in x. The line of code x = (x>>8) then right shifts x by one byte. (Thus, as the loop runs, at each iteration the three different least significant bytes of x are "in place" to be XORed with the mask. So the XOR to compute is:

```
10000010      (bits 1 and 7 are on)
00100010      (bits 9-8=1 and 13-8=5 are on)
00100010      (bits 17-16 = 1 and 21-16 = 5 are on)
------------
```

10000010 (converted back to decimal this is $2^7 + 2^1 = 130$.)

130

Grading: 2 pts for recognizing that bytes are being XORed, 3 pts for the correct computation of the XOR and conversion to base 10.

2) (6 pts) Let P = [3 2   12   8   1 7   11   6   4   10   5   9] be a permutation matrix similar to the permutation matrix P in DES, which could be applied to an input of 12 bits. Calculate the corresponding inverse permutation, IP.

Just look where in P the value 1 is, then 2, then 3, etc. 1 is in position 5, 2 is in position 2, 3 is in position 1, 4 is in position 9 and so forth. This yields the answer:

IP = [5, 2, 1, 9, 11, 8, 6, 4, 12, 10, 7, 3]

Grading: ½ pt per slot, round down

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. 1 pt for correct answers in decimal or HEX.)

(a) $S_1(010100)$ = 0110, S-box 1, row = 00 = 0, col = 1010 = 10, S1[0][10] = 6 = 0110_2

(b) $S_3(001011)$ = 0100, S-box 3, row = 01 = 1, col = 0101 = 5, S3[1][5] = 4 = 0100_2

(c) $S_4(111100)$ = 1000, S-box 4, row = 10 = 2, col = 1110 = 14, S4[2][14] = 8 = 1000_2

(d) $S_8(111011)$ = 0101, S-box 8, row = 11 = 3, col = 1101 = 13, S8[3][13] = 5 = 0101_2

Grading: ½ if correct decimal answer, 2/2 if correct binary answer, 0/2 otherwise

4) (6 pts) In the DES Key Schedule algorithm, let the bit in position 1 of C_0 be b. In which position will b appear in C_1, C_2, C_3, C_4, C_5 and C_6? Note: for the purposes of this question, use one based indexing. As a hint, the valid answers for each of the six answers all lie in between 1 and 28, inclusive.

Position of b in C_1: 28 , left shift of 1 from position 1 goes to position 28

Position of b in C_2: 27, left shift of 1 from position 28 goes to position 27

Position of b in C_3: 25, left shift of 2 from position 27 goes to position 25

Position of b in C_4: 23, left shift of 2 from position 25 goes to position 23

Position of b in C_5: 21, left shift of 2 from position 23 goes to position 21

Position of b in C_6: 19, left shift of 2 from position 21 goes to position 19

Grading: 1 pt for each all or nothing, so if the first one's off, it's likely the rest will be also.

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:

01	23	45	67
89	AB	CD	EF
A0	B2	C2	D3
E4	F5	69	78

7C	26	6E	85
A7	62	BD	DF
E0	37	25	66
69	E6	F9	BC

Grading: ½ per entry, 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 4, column 3, right AFTER the MixCols step? Express your answer as **2 HEX characters.** (Note: Max credit for correctly computing the wrong entry is 3 points out of 10. So be careful!!!)

01	88	AD	63
A6	23	72	E7
B7	FF	EB	86
93	BC	D7	2F

Answer = 03 x AD + 01 x 72 + 01 x EB + 02 x D7

```
03 x AD = 02 x AD + 01 x AD                      So 03 x AD   = 0100 0001 (02 x AD)
          02 x AD = 1010 11010 = 0101 1010 +                   1010 1101 (01 x AD) +
                                 0001 1011                     ------------
                                 -------------                 1110 1100 (EC)
                                 0100 0001

02 x D7 = 1101 01110 = 1010 1110
                     + 0001 1011
                       -------------
                        1011 0101 (B5)
```

Thus, final answer is EC + 72 + EB + B5 = (EC+EB) + (72+B5) = (07) + (C7) = **C0**

Grading: 2 pts writing out correct sum of products, 4 pts for 03 x AD, 2 pts for 02 x D7, 2 pts for completing the final XOR

7) (6 pts) We spent some class time investigating multiplication in the AES field. Using the information given in lecture, calculate the product 06 x EB in the field defined for AES. **Please express your answer as 2 HEX characters.**

06 x EB = (04 + 02) x EB
Note: 04 x EB = 02 x (02 x EB), due to polynomial interpretation of AES bytes.

```
02 x EB = 02 x 1110 1011 = 1110 10110 = 1101 0110 +
                                        0001 1011
                                        -------------
                                        1100 1101        (CD)
```

```
04 x EB = 02 x CD = 1100 11010 = 1001 1010 +
                                 0001 1011
                                 -------------
                                 1000 0001               (81)
```

Final answer = CD + 81 = **4C**

Grading: 2 pts for 02 x EB, 3 pts for 04 x EB, 1 pt for final XOR

8) (1 pt) The Orion spacecraft, part of NASA's Artemis program, is named after what constellation?

Orion (Give to all)