Fall 2026 CIS 3362 Exam #2: Bitwise Operators, DES, AES Solutions

Date: 10/14/2026

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

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

What is the corresponding IP^{-1} matrix?

Solution

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

Grading: 1/2 pt per entry, round down to nearest integer.

2) (10 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.**)

Solution

(a) $S_2(100101)$ = **1010** , $S_2[3][2] = 10$, converted to binary on the left.

(b) $S_4(000110)$ = **0011** , $S_4[0][3] = 3$, converted to binary on the left.

(c) $S_6(110110)$ = **1010** , $S_6[2][11] = 10$, converted to binary on the left.

(d) $S_7(010101)$ = **0101** , $S_7[1][10] = 5$, converted to binary on the left.

(e) $S_8(111101)$ = **0110** , $S_8[3][14] = 6$, converted to binary on the left.

Grading: 2 pts per answer, 1 pt if correct decimal or hex, 2 pts only if correct binary

3) (12 pts) Consider the task of writing a function (**in C**) that takes in an array of unsigned ints, each of which are 32 bits and makes the following calculation: for each integer, split the integer into two halves, the right 16 bits (least significant) call these R_i and the left 16 bits (most significant) call these L_i, and compute R_i xor L_i. Then xor each of these results for each integer and return the result. Note that I chose unsigned int because when you right shift an unsigned integer that starts with a 1 in its most significant bit, those bits get filled in with 0s, which is mildly helpful for this question. (For example, if our message array had two integers in it where the first integer had bits 0, 1, 5, 14, 16 and 18 on, and our second integer had bits 3, 21 and 30 on, then the function should return the value 14 because $14 = 2^1 + 2^2 + 2^3$, because bits 0 and 16 cancel out (16 is the least significant bit of the Left side), bits 5 and 21 cancel out, and bits 14 and 30 cancel out. This leaves bits 1, 18 and 3 on. Remember that 18 is the place 2^2 on the left side, so the final result is 14 for this computation. Please complete the task below. Much more room is provided than necessary.

```
unsigned int xorSignature(unsigned int* message, int length){

    unsigned int right = (1<<16)-1;          // 2 pts

    unsigned int res = 0;                    // 1 pt
    for (int i=0; i<length; i++) {           // 1 pt

        // 7 pts - 1 pt LHS, 1 pt ^, 3 pts right, 2 pts left
        res = res ^ (right&message[i]) ^ (message[i]>>16);
    }

    return res;                              // 1 pt

}
```

4) (8 pts) Consider the DES Key Schedule algorithm. Imagine that in the middle of the algorithm, we have the following values for C_6 and D_6, in binary:

C_6 = 0001 1001 0111 0010 1111 0111 1010
D_6 = 1011 1100 0000 1010 1110 1101 1011

Please show your work and determine the first 16 bits of K_7, the round 7 key. (Note: since random luck will get 8 bits correct, the scoring on this question will simply be max(0, correctbits-8).)

Solution

Note that LS_6 is 2 bits, so we have

C_7 = 01 1001 0111 0010 1111 0111 1010 00
D_7 = 11 1100 0000 1010 1110 1101 1011 10, now rewrite grouped in 4s:

C_7 = 0110 0101 1100 1011 1101 1110 1000
D_7 = 1111 0000 0010 1011 1011 0110 1110

Now, apply PC-2, which starts 14, 17, 11, 24, ... and grab those particular bits:

0 1 0 0 0 0 1 0 1 1 1 1 1 0 0 0

Grading: max(0, total – 8)

5) (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:

22	87	C5	7B
37	6E	D9	5F
8A	D4	2F	C6
B2	C1	F3	DF

93	17	A6	21
9A	9F	35	CF
7E	48	15	B4
37	78	0D	9E

Grading: 1 pt per row, row has to be completely correct to get the point.

6) (4 pts) Take your result from above and execute the ShiftRows step on it, showing the result below:

93	17	A6	21
9F	35	CF	9A
15	B4	7E	48
9E	37	78	0D

Grading: 1 pt per row, row has to be completely correct to get the point.

7) (8 pts) Consider the process of AES Key Expansion. Imagine that we have:

w[28] = F3 76 5B 19 (in hex)
w[31] = B3 C2 56 D0 (in hex)

Calculate w[32] and express your answer as **8 HEX characters.** (Show your answer after each step designated below:

temp	= **B3 C2 56 D0**	**1 pt**
After RotWord	= **C2 56 D0 B3**	**1 pt**
After SubWord	= **25 B1 70 6D**	**1 pt**
Rcon(**8**)	= **80 00 00 00**	**1 pt**
After XOR w/Rcon	= **A5 B1 70 6D**	**1 pt**
w[**28**]	= **F3 76 5B 19**	**1 pt**
Final Answer	= **56 C7 2B 74**	**2 pts**

8) (10 pts) In the AES Field GF(2^8) with the irreducible polynomial $x^8 + x^4 + x^3 + x + 1$, what is the product of $(x^6 + x^3)$ and $(x^5 + x^3 + x^2 + 1)$? Express your answer in **2 HEX characters.**

Solution

$(x^6 + x^3)(x^5 + x^3 + x^2 + 1) = x^{11} + x^9 + x^8 + x^6 + x^8 + x^6 + x^5 + x^3$

The highlighted part cancels out, so our answer is equivalent to

$x^{11} + x^9 + x^5 + x^3 = x^8(x^3 + x) + x^5 + x^3 \equiv (x^4 + x^3 + x + 1)(x^3 + x) + x^5 + x^3$

$= (x^7 + x^6 + \mathbf{x^4 + x^3}) + (\mathbf{x^5 + x^4} + x^2 + x) + \mathbf{x^5 + x^3}$

$\equiv x^7 + x^6 + x^2 + x \bmod (x^8 + x^4 + x^3 + x + 1)$

In binary this polynomial is 1100 0110, converted to HEX is C6.

C6

Grading: 3 pts regular FOIL
2 pts cancel x^8, x^6
3 pts reduce x^{11} and x^9
2 pts getting to final answer (give 1 pt if in binary only 2 pts if in HEX)

9) (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 3, column 2 (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	9B	93	19
A4	49	E5	E3
B9	AB	4F	46
47	E2	C7	6F

Solution

The desired product is 01 x 9B + 01 x 49 + 02 x AB + 03 x E2.

```
01 x 9B = 9B
01 x 49 = 49

02 x AB = 1010 1011 0 = 0101 0110
                        ^  1 1011
                        ---------
                        0100 1101 (4D)

03 x E2 = (01 + 02) x E2 =
          01 x E2 = E2

          02 x E2 = 1110 0010 0 = 1100 0100
                                  ^  1 1011
                                  ---------
                                  1101 1111 (DF)

Thus, 03 x E2 = E2 + DF = 3D

Final answer is (9B + 49) + (4D + 3D) = D2 + 70 = A2
```

A2

Grading: Max grade wrong product = 2 out of 10
02 x AB = 2 pts, 03 x E2 = 4 pts, XOR everything = 3 pts, expressing in HEX 1 pt

10) (1 pt) In 1947 on this day, Chuck Yeager broke the sound barrier. This means he traveled faster than the speed of what?

Sound (Give to All)