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

Date: 10/14/2026

Name : _____

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?

___ ___ ___ ___

___ ___ ___ ___

___ ___ ___ ___

___ ___ ___ ___

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.**)

(a) $S_2(100101)$ = _____

(b) $S_4(000110)$ = _____

(c) $S_6(110110)$ = _____

(d) $S_7(010101)$ = _____

(e) $S_8(111101)$ = _____

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){

}
```

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).)

___ ___ ___ ___ ___ ___ ___ ___ ___ ___ ___ ___ ___ ___ ___ ___

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

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

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 = _____

After RotWord = _____

After SubWord = _____

Rcon(___) = _____

After XOR w/Rcon = _____

w[____] = _____

Final Answer = _____

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.**

____ ____

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

___ ___

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

_____

Scratch Page – Please clearly mark any work on this page you would like graded.