Fall 2025 CIS 3362 Homework #4: DES, AES
Due: Check WebCourses for the due date.

1) (30 pts) The IP matrix in DES permutes the bits in the block of bits being encrypted. We can write code to apply IP (or any permutation matrix) to an unsigned long long storing 64 bits in C. Please use bitwise operators to complete the function, applyPerm, in attached file, question1.c. (We will call your function with several input values and check if the output values are correct.)

2) (6 pts) The input to the expansion matrix E in DES, expressed in hexadecimal is 3F6BD297. What is the output? Please express your answer in **hexadecimal** and put a little space between each group of **2** hex characters.

3) (8 pts) Consider a portion of a single DES round where the input (expressed in HEX) to S boxes S_1, S_2, S_3, S_4 S_5, S_6, S_7, and S_8 is `13579BDFC840`. What are the 32 bits of output from the S-boxes? Express your result in **binary (so 32 separate bits)**. (Note: Partial credit on this question will be limited for obvious reasons, so double check your answers.)

4) (12 pts) In the DES Key scheduling algorithm, a buffer has to be cyclically left-shifted. Complete the function cyclicLeftShift, in the attached file, question4.c, so that it uses bitwise operators to return the value of the input buffer when it's cyclically left shifted by b bits. (We will call your function with several input values and check if the output values are correct.)

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:

29	76	0A	1B
8C	3D	4E	5F
A3	B7	C2	D9
E0	F5	14	68

6) (4 pts) Let the state matrix to AES right before the ShiftRows step be your answer from problem 5. Show the state of the matrix right AFTER the ShiftRows step. (This will be graded solely based on what your answer to problem 5 was. You can get this one correct even if you got problem 5 incorrect.)

7) (10 pts) Consider the process of AES Key Expansion. Imagine that we have:

w[28] = B5 2F 3C 97 (in hex)
w[31] = 1E 06 A8 4D (in hex)

Calculate w[32], showing each of the following intermediate results: RotWord(temp), SubWord(RotWord(temp)), Rcon[i/4], and the result of the XOR with Rcon[i/4]

RotWord	SubWord	Rcon[i/4]	XOR	FinalResult

8) (12 pts) In class we discussed multiplication in the AES field GF(2^8) with the irreducible polynomial $x^8 + x^4 + x^3 + x + 1$. Based on this discussion, derive the answer for the calculation of 14 x E6. Display your final result with two hexadecimal characters.

9) (10 pts) Let the input to the MixCols (during AES encryption) be $\begin{bmatrix} B5 & 34 & 29 & 06 \\ A6 & 19 & 79 & 97 \\ 63 & F5 & 4C & C2 \\ DB & D2 & FD & A3 \end{bmatrix}$.

What's the output in row 4 col 1? (The matrix by which to "multiply" is $\begin{bmatrix} 02 & 03 & 01 & 01 \\ 01 & 02 & 03 & 01 \\ 01 & 01 & 02 & 03 \\ 03 & 01 & 01 & 02 \end{bmatrix}$.)