Fall 2026 CIS 3362 Homework #4: DES, AES
Due: Check WebCourses for the due date.

1) (10 pts) Show the result of applying the IP to the following input block represented in hexadecimal: 6A3B 05C9 D841 FE27. Express the final result in HEX. Show your 64 bits written out in order in your work and indicate the output 64 bits and their conversion to HEX.

2) (10 pts) The input to the expansion matrix E in DES, expressed in hexadecimal is 89AB5F62. What is the output? Please express your answer in **hexadecimal** and put a little space between each group of **2** hex characters.

3) (10 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 `2345 9876 CDEF`. 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) (20 pts) Use the posted code, DES.java and the corresponding text file destables.txt, to encrypt the following text:

```
This is
a test,
for the
2026 CIS
 3362 DE
S Assign
ment.(^)
```

using the following key in HEX: `BC19 C7AC 23F1 9E70`

Each line above has exactly 8 characters. To encode, encode each character into 8 bits according to its Ascii value. Your ciphertext will be binary, when converted back to Ascii many of the characters will not printable, so express your output in hexadecimal (16 HEX characters per block.)

This question is testing your ability to take the posted code an modify/use it to solve the task at hand.

Explain the modifications you made to the code in your write up and provide the final answer. It's okay to do some portion of the work by hand. (Say the program produces output in binary, then you may either manually convert it to hex, or write code to do so. Either is fine, just state in your write up what you did and if you did write code, include it.)

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:

63	9A	45	27
C8	02	E9	F6
24	68	AC	E0
31	75	B9	FD

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[36] = 49 C0 E7 58 (in hex)
w[39] = 23 16 AB DF (in hex)

Calculate w[40], 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 08 x 9E. Display your final result with two hexadecimal characters.

9) (16 pts) Let the input to the MixCols (during AES encryption) be $\begin{bmatrix} B5 & 34 & 29 & A6 \\ A6 & 19 & 79 & 97 \\ 63 & F5 & 4C & C2 \\ DB & D2 & FD & A3 \end{bmatrix}$.

Working by hand, show the work and output in both row 1, column 4 AND row 2, column 3? (So 8 points for each.)

(The matrix by which to "multiply" is $\begin{bmatrix} 02 & 03 & 01 & 01 \\ 01 & 02 & 03 & 01 \\ 01 & 01 & 02 & 03 \\ 03 & 01 & 01 & 02 \end{bmatrix}$.)