Fall 2024 CIS 3362 Homework #4: DES, AES
Due: Check WebCourses for the due date.

1) Consider creating a DES-like block cipher with a block size of 16. Assume that the cipher has a fixed matrix IP, just like DES, that operates exactly as DES's IP matrix. Given the IP matrix shown below, calculate the corresponding matrix, IP^{-1}.

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

$$IP^{-1} =$$

2) The input to the expansion matrix E in DES, expressed in hexadecimal is B4F392C6. What is the output? Please express your answer in **hexadecimal** and put a little space between each group of **2** hex characters. Use words to explain how you arrived at the answer so that the grader can verify that the answer is correct **for the right reason.**

3) 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 2413ACBD5F6E. 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) Consider calculating the round 16 key in DES. Given that the input key, with odd parity bits, when described in HEX is **"C761 4592 BCC2 5D38"**, **determine the first 10 bits of the round 1 key. Credit will only be given if appropriate work is shown since it's easy to randomly put bits down and get around half of them. I'll decide what appropriate work is!!!**

5) In the past I offered a DES challenge where I gave students some bits of the 56-bit key and they had to brute force the rest. Consider that most of the students in the course take one of two approaches to break the key, exemplified by Student X and Student Y below:

(a) Student X has decided to use the professor's slow Java implementation (so no time to code the DES portion of the code) and add the brute force mechanics (this takes 1 hour), and then check each key at a rate of 200,000 keys per second.

(b) Student Y has decided to rewrite the professor's code in C++ and write the corresponding brute force mechanics (takes 2 days/48 hours, including adding the brute force mechanics), and then check each key at a rate of 2,000,000 keys per second.

The professor would like for both Student X and Student Y’s approaches to take the same total time (or as close as possible). How many bits of the key should the professor reveal?

6) 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
8F	9E	AD	BC
40	51	62	73
FC	EB	DA	98

7) Let the state matrix to AES right before the ShiftRows step be your answer from problem 7. Show the state of the matrix right AFTER the ShiftRows step. (This will be graded solely based on what your answer to problem 7 was. You can get this one correct even if you got problem 7 incorrect.)

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

w[32] = A3 B4 C7 D9 (in hex)
w[35] = 05 18 2E 6F (in hex)

Calculate w[36], 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

9) 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 07 x 9D. Display your final result with two hexadecimal characters.

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

What's the output in row 3 col 2? (The matrix by which to "multiply" is $\begin{bmatrix} 02 & 03 & 01 & 01 \\ 01 & 02 & 03 & 01 \\ 01 & 01 & 02 & 03 \\ 03 & 01 & 01 & 02 \end{bmatrix}$.)