CIS 3362 Homework #4: Symmetric Cipher Tracing
Due: Check WebCourses for the due date.

1) Consider a cipher that uses a 16 bit key and 16 bit blocks. Let A and B both be permutations matrices used in the cipher, assuming that A and B are expressed in a similar manner to how IP is expressed in DES. Let C be a matrix that represents the equivalent permutation to applying A, followed by applying B. (Thus, C(x) = B(A(x)), where x is a 16 bit input.) Determine C given the matrices A and B below:

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

2) Imagine a DES-like cipher with a block size of 16 with the following IP matrix:

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

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

3) If the input into all 8 S-boxes in DES is 8df63098e724, what is the output? Please express your output in 8 hexadecimal characters.

4) The first part of the function F in a round of DES expands the 32-bit input (from the right half of the previous round) to 48 bits. If this input, in HEX to the function F is BF8293E6, what is the output of the expansion matrix. Express your answer as 12 hexadecimal characters.

5) In the specification of DES, the key is represented as 64 bits, of which some are parity bits. Label all the bits (including parity bits) as k_1, k_2, ..., k_{64}. If you knew the values of k_1 through k_{16}, but had to perform a brute force search through the other bits of the key, how long, in the worst case, would it take you to find the key, given that you can search through 2^{20} keys in one second? Please express your answer in days, rounded to the nearest day.

6) Let the input to the MixCols (during AES encryption) be $\begin{bmatrix} A0 & 74 & 65 & 96 \\ 2B & 8D & 2E & E3 \\ 99 & 1F & C8 & 37 \\ C5 & E5 & F7 & BB \end{bmatrix}$.

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

7) In the key expansion algorithm of AES, if w[26] = 8EFA5329 and w[23] = 7EE826D3, what is w[27]?

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

w[36] = 3A 74 E5 8D (in hex)
w[39] = 8F 17 60 C2 (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

9) Without examining all entries in the 16 round key schedule of DES, determine whether or not each number (which represents a bit location in the original key in each of the 16 boxes labeled "Round 1" through "Round 16") appears the exact same number of times collectively in the 16 boxes. (As an example, 10 appears in round except rounds 4, 12 and 14, so it appears 13 times.) Give proof of your answer.

10) Consider an AES plaintext of $\begin{bmatrix} 01 & 89 & FE & 76 \\ 23 & AB & DC & 54 \\ 45 & CD & BA & 32 \\ 67 & EF & 98 & 10 \end{bmatrix}$ with a key of 128 1s. Show the state matrix after the shift rows step in Round 1.