CIS 3362 Homework #4: Hill Cipher, Bitwise Operators, DES, AES
Due: Check WebCourses for the due date.

Directions: To be done in pairs. If you can't find someone to work with, you must submit individually. When you submit, please CLEARLY mark both group members on each document you submit.

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:

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

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

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

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

3) If the input into all 8 S-boxes in DES is 1245789ABCDF, 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 59E6BA91, 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_{24}, 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 hours, minutes and seconds.

6) Let the input to the MixCols (during AES encryption) be $\begin{bmatrix} A0 & 74 & 65 & 96 \\ 2B & 8D & 2E & E3 \\ 99 & 1F & C8 & 87 \\ C5 & E5 & F7 & BB \end{bmatrix}$.

What's the output in row 3 col 4? (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[34] = BB3A7920 and w[31] = C659D034, what is w[35]?

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

w[28] = B5 13 2F 76 (in hex)
w[31] = F4 9A 0D 8C (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

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) Using the code, AES.java, posted in the course examples, write a program (preferably in Java, but C, C++ and Python will be accepted as well), that prints out a 256 x 256 chart which has the results of every possible byte multiplication in the AES field. Your program should output 256 rows, where the i^{th} row stores the products with byte value i-127. Your output should express each value as 2 hex chars followed by a space. (So, each row should have 256 x 3 = 768 characters on it, followed by a new line character.) The hex letters should be lower case and leading 0s should be printed. In Java, we can accomplish this as follows:

```
System.out.printf("%02x ", byteToBePrinted);
```

Here is the beginning of the output of the few lines:

```
9b 03 82 28 a9 31 b0 7e ff 67
03 9e 1c bf 3d a0 22 fd 7f e2
82 1c 9f 3b b8 26 a5 75 f6 68
28 bf 3b 8a 0e 99 1d e0 64 f3
```