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}.

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

$$IP^{-1} =$$

2) The input to the expansion matrix E in DES, expressed in hexadecimal is A39047FC. What are the first 24 bits of output? Please express your answer in bits and put a little space between each group of **6** bits. Use words to explain how you arrived at the answer so that the grader can verify that the answer is correct **<u>for the right reason.</u>**

3) Consider a portion of a single DES round where the ***<u>last</u>*** 24 bits of input (expressed in HEX) to S boxes S_5, S_6, S_7, S_8 is `70D6B9`. What are the 16 bits of output from those 4 S-boxes? Express your result in binary. (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 **`"A197 47F2 E9C1 B35D"`**, **determine the first 10 bits of the round 16 key.** (Note: While it looks like an inordinate amount of calculation is necessary here, it turns out that a particular observation that I might off-hand in class makes this calculation very quick. I would strongly not recommend trying to "brute force" this question. Rather, I'd recommend only doing it if you make the observation that allows you to do this question in a minute or so.) **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 20 of the 56 bits, so that they would have to brute force the remaining 36 bits. Consider a student X, who is approaching the assignment and has two options for tackling it:

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

(b) 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.

How much time (please answer in days/hours/minutes/seconds) would each option take? (Please use a calculator to do the arithmetic but set up the fraction on paper.) What option should the student choose?

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:

5F	02	37	1A
B4	4B	C6	7E
83	29	D8	95
F1	EC	6D	A0

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[24] = 01 32 45 76 (in hex)
w[27] = 89 BA CD FE (in hex)

Calculate w[28], 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 26. Display your final result with two hexadecimal characters.

10) 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 $\begin{bmatrix} 02 & 03 & 01 & 01 \\ 01 & 02 & 03 & 01 \\ 01 & 01 & 02 & 03 \\ 03 & 01 & 01 & 02 \end{bmatrix}$.)