# CIS 3362 Homework #3: Light Coding Group - DES, AES

**Due Date: Check Webcourses**

**Directions: Please work out the following problems by hand, showing each step of your process. While this homework is tedious, after you are finished with it, you'll understand the mechanics of each step in both DES and AES.**

1) Let b = 93de8067f5942ca1, a plaintext block (expressed in hexadecimal). What is IP(b)?

2) Using the same block b shown in question #1, calculate $IP^{-1}(b)$.

3) The Feistel function in DES takes in one 32 bit argument (half of the bits in the process of encryption) and a 48 bit argument (the key for that particular round). If $R_{i-1}$ = 94e2d671 (in hex) and $K_i$ = b57c809a743e, calculate $F(R_{i-1}, K_i)$. Your calculation should show the following steps: the use of the expansion matrix E, the XOR with the key, the S-box substitution and the application of the permutation matrix P.

4) Given the following state matrix in AES, show what it would look like after applying the sub bytes step?

| | | | |
|---|---|---|---|
| 3E | 1E | 32 | 10 |
| 67 | 96 | FF | 65 |
| A8 | 6B | AB | 9E |
| 5A | 06 | 9C | 43 |

5) Now, apply the shift rows operation to your result from question 4, what is the resulting state matrix?

6) Consider the following Mix Columns step in AES:

$$\begin{bmatrix} 02 & 03 & 01 & 01 \\ 01 & 02 & 03 & 01 \\ 01 & 01 & 02 & 03 \\ 03 & 01 & 01 & 02 \end{bmatrix} \begin{bmatrix} 79 & 45 & A3 & C4 \\ 28 & 8E & 59 & D9 \\ A5 & C1 & 9C & 21 \\ 96 & F6 & C5 & 18 \end{bmatrix}$$

Calculate the four following entries: (a) row 1, column 2
(b) row 2, column 4
(c) row 3, column 3
(d) row 4, column 1