# AES Problem

Starting with a 128 bit block of plaintext represented by

**2d 5f 34 30 fe 1f 1e 3a 11 22 33 44 55 66 77 88**

And an initial 128 bit key given as

**f1 e2 d3 a4 c5 b6 f7 e8 c9 a0 44 55 66 77 11 22**

A) Create the initial input state matrix

B) Develop the first four words of the key expansion matrix

C) Show the values of the first column of the state matrix

  i. after the initial AddRoundKey operation

  ii. the S Box transformation

  iii. a Mix Column operation

MixColumn replaces a 4-octet column with another 4-octet column. This operation can be implemented with a single table containing 256 4-octet columns. Each of the octets in the column is used as an index to retrieve a column from the table. Each column retrieved from the table is rotated vertically so that its top octet is in the same row as the input octet and the four rotated columns are XORed together to produce the output column.

Hint: Using an online XOR calculator would help expedite the calculations