## EECE 455/632 – Cryptography and Network Security

## Assignment

# CHAPTER 5 - AES

**Question #1**

a) What is the inverse of {7B} in GF($2^8$)?

b) Verify the entry for {7B} in the AES S-Box

**Question #2**

Using the key `ABACABAC ABACABAC ABACABAC ABACABAC `, show the first eight words of the AES (128 bits) key expansion.

**Question #3**

Given the Plaintext in Hex: {A1B2C3D4E5F60718292A3B4C5D6E7F80};

And given the Key in Hex below (*3**0 = 0010 0000***):

{3030303030303030303030303030303030303030303030303030303030303030}

For the first round of **AES**:

a) Show the original contents of **State**, displayed as a 4x4 Matrix

b) Show the value of **State** after initial **ADD ROUND KEY**

c) Show the value of **State** after initial **SUBSTITUE BYTES**

d) Show the value of **State** after initial **SHIFT ROWS**

e) Show the value of **State** after initial **MIX COLUMNS**

**Question #4**

Compute the outcome of the **AES** Mix-Columns transformation for the sequence of input bytes: **4D 90 4A D8**.