UEE4611 Assignment #5, 2020 due April 30

1. (a) Determine the multiplicative inverse of $\{02\}$ in $GF(2^8) = \mathbb{Z}_2[x]/\langle x^8 + x^4 + x^3 + x + 1\rangle$. (10%)

   (b) Verify the entry for $\{02\}$ in the S-box. (10%)

2. Consider the encryption algorithm of AES. Given the plaintext

$$\{0F0E0D0C0B0A09080706050403020100\}$$

and the key

$$\{02020202020202020202020202020202\},$$

   (a) Show the original contents of **State**, displayed as a 4×4 matrix. (5%)

   (b) Show the value of **State** after initial AddRoundKey. (5%)

   (c) Show the value of **State** after SubBytes. (5%)

   (d) Show the value of **State** after ShiftRows. (5%)

   (e) Show the value of **State** after MixColumns. (5%)