Problems

5.1 In the discussion of MixColumns and Inverse MixColumns, it was stated that

\[ b(x) = a^{-1}(x) \mod (x^4 + 1) \]

where \( a(x) = \{03\}x^3 + \{01\}x^2 + \{01\}x + \{02\} \) and \( b(x) = \{0B\}x^3 + \{0D\}x^2 + \{09\}x + \{0E\} \). Show that this is true.
5.2 a. What is $\{01\}^{-1}$ in GF($2^8$)?
b. Verify the entry for $\{01\}$ in the S-box.

5.3 Show the first eight words of the key expansion for a 128-bit key of all zeros.

5.4 Given the plaintext $\{000102030405060708090A0B0C0D0E0F\}$ and the key $\{010101010101010101010101\}$,
a. Show the original contents of $\text{State}$, displayed as a $4 \times 4$ matrix.
b. Show the value of $\text{State}$ after initial AddRoundKey.
c. Show the value of $\text{State}$ after SubBytes.
d. Show the value of $\text{State}$ after ShiftRows.
e. Show the value of $\text{State}$ after MixColumns.

5.5 Verify Equation (5.11). That is, show that $x^4 \mod (x^4 + 1) = x^4 \mod 4$.

5.6 Compare AES to DES. For each of the following elements of DES, indicate the comparable element in AES or explain why it is not needed in AES.
a. XOR of subkey material with the input to the $f$ function
b. XOR of the $f$ function output with the left half of the block
c. The $f$ function
d. Permutation $P$
e. Swapping of halves of the block

5.7 In the subsection on implementation aspects, is it mentioned that the use of tables helps thwart timing attacks. Suggest an alternative technique.

5.8 In the subsection on implementation aspects, a single algebraic equation is developed that describes the four stages of a typical round of the encryption algorithm. Provide the equivalent equation for the tenth round.

5.9 Compute the output of the MixColumns transformation for the following sequence of input bytes "AB CD". Apply the InvMixColumns transformation to the obtained result to verify your calculations. Change the first byte of the input from "AB" to "AA"; perform the MixColumns transformation again for the new input, and determine how many bits have changed in the output. *Note: You can perform all calculations by hand or write a program supporting these computations. If you choose to write a program, it should be written entirely by you; no use of libraries or public domain source code is allowed in this assignment.*

5.10 Use the key 1010 0111 0111 1011 to encrypt the plaintext "ok" as expressed in ASCII, that is 0110 1111 0110 1011. The designers of S-AES got the ciphertext 0000 0111 0111 1000. Do you?

5.11 Show that the matrix given below, with entries in GF($2^4$), is the inverse of the matrix used in the MixColumns step of S-AES.

$$
\begin{pmatrix}
  x^3 + 1 & x \\
  x & x^3 + 1
\end{pmatrix}
$$

5.12 Carefully write up a complete decryption of the ciphertext 0000 0111 0111 1000, using the key 1010 0111 0011 1011 and the S-AES algorithm. You should get the plaintext we started with in Problem 5.10. Note that the inverse of the S-boxes can be done with a reverse table lookup. The inverse of the MixColumns step is given by the matrix in the previous problem.

### Programming Problems

5.13 Create software that can encrypt and decrypt using S-AES. Test data: a binary plaintext of 0111 0111 0111 0111 and a binary key of 1010 0111 0011 1011 should give a binary ciphertext of 0000 0111 0111 1000 less ecb $\$$$. Decryption should work correspondingly.

5.14 Implement a differential cryptanalysis attack on 1-round S-AES.