Homework Assignment # 7

Due Date: Wednesday, November 1

As accompanying information to the lecture and as aid for the problems in this assignment, read the "Algorithm Specifications" of Rijndael which can be found at
`http://csrc.nist.gov/encryption/aes/round2/r2algs.htm#Rijndael`
However, this is *not* meant as a formal reading assignment.

1. Compute $A \cdot B$ in $GF(2^4)$ with $P(x) = x^4 + x + 1$
   (a) for $A(x) = x^2 + 1$, $B(x) = x^3 + x^2 + 1$,
   (b) for $A(x) = x^2 + 1$, $B(x) = x + 1$.

2. Can none, one, or both of the following polynomials be used for building the field $GF(2^3)$? Hint: Check whether those polynomials can be factored in polynomials with smaller degree.
   (a) $x^3 + x^2 + x + 1$
   (b) $x^3 + x^2 + 1$

3. We consider the field $GF(2^4)$, with $P(x) = x^4 + x + 1$ being the irreducible polynomial. Find the inverse of $A(x) = x$ and $B(x) = x^2 + x$. Verify your answer by multiplying the inverses you determined by A and B, respectively.

4. The MixColumn transformation of Rijndael consists of a matrix-vector multiplication in the field $GF(2^8)$ with $P(x) = x^8 + x^4 + x^3 + x + 1$. Let $b = (b_7 x^7 + \ldots + b_0)$ be one of the (four) input bytes to the vector-matrix multiplication. Each input byte is multiplied with the constants 01, 02, and 03. Your task is to provide exact equations for computing those three constant multiplications. We denote the result by $d = (d_7 x^7 + \ldots + d_0)$.
   (a) Equations for computing the 8 bits of $d = 01 \cdot b$.
   (b) Equations for computing the 8 bits of $d = 02 \cdot b$.
   (c) Equations for computing the 8 bits of $d = 03 \cdot b$.

   Note: The Rijndael specification uses "01" to represent the polynomial 1, "02" to represent the polynomial x, and "03" to represent $x + 1$. See also Section 2.1.2 of the Rijndael specification for more examples.

5. We look now at the gate (or bit) complexity of the MixColumn function, using the results from problem 4. We recall from the discussion of stream ciphers that a 2-input XOR gate performs a $GF(2)$ addition.

   (a) How many 2-input XOR gates are required to perform one constant multiplication by 01, 02, and 03, respectively, in $GF(2^8)$.

   (b) What is the over-all gate complexity of a hardware implementation of one matrix-vector multiplication?

   (c) What is the over-all gate complexity of a hardware implementation of the entire Diffusion Layer? We assume permutations require no gates.

6. What is the output of the ByteSub transformation for the input

   (a) 01 (hex)

   (b) 12 (hex)

   Note that you have to represent those values first as polynomials in $GF(2^8)$. The MSB of each byte represents the x^7 coefficient etc.