2. Assignment: Arithmetic in $\mathbb{F}_{256}[y]$  
(Due: Wednesday, 12 November 2008, 13:40, b-it bitmax)

Exercise 2.1 (MixColumns). (12 points)

The MixColumns-step of the AES-algorithm takes place in the ring

$$S = \mathbb{F}_{256}[y]/\langle y^4 + 1 \rangle.$$ 

(i) The ring $S$ is not a field. In particular, there are nonzero elements in $S$ without a multiplicative inverse. Give an example and explain how you could check that property. 

(ii) The output $b_3, b_2, b_1$ and $b_0$ of the MixColumns-step for a column with entries $a_3, a_2, a_1$ and $a_0$ is determined by the product

$$b_3y^3 + b_2y^2 + b_1y + b_0 = (02 + 01y + 01y^2 + 03y^3) \cdot (a_3y^3 + a_2y^2 + a_1y + a_0).$$ 

Expand the product over $\mathbb{F}_{256}[y]$, reduce it modulo $y^4 + 1$ and collect the terms with equal powers of $y$ to obtain equations for $b_3, b_2, b_1$ and $b_0$. 

(iii) Find a $4 \times 4$-matrix $M$ with entries from $\mathbb{F}_{256}$ to express this multiplication as a matrix-vector product

$$\begin{pmatrix} b_0 \\ b_1 \\ b_2 \\ b_3 \end{pmatrix} = M \cdot \begin{pmatrix} a_0 \\ a_1 \\ a_2 \\ a_3 \end{pmatrix}.$$ 

(iv) Use this matrix-vector product to perform the MixColumns-operation on the following state of AES:

$$\begin{bmatrix} 00 & 00 & 00 & 00 \\ 7A & 00 & 00 & 00 \\ 01 & 00 & 01 & 00 \\ 00 & 00 & 00 & AA \end{bmatrix}$$

(v) The InvMixColumns-operation is the inverse of MixColumns. From exercise 1.3 (iii) you know that the product of $02 + 01y + 01y^2 + 03y^3$ with $0B y^3 + 0D y^2 + 09 y + 0E$ is $01$ in $S$. Use this information to write down the InvMixColumns-operation on a column $b$ in matrix-vector-notation.
**Exercise 2.2** (Repeated-Squaring). (8 points)

For a given positive integer $N$ we consider the set $\mathbb{Z}_N$ of all residues modulo $N$, i.e.

$$\mathbb{Z}_N = \{0, 1, \ldots, N - 1\}.$$  

On this set we can add, multiply and raise to powers, by simply performing the well-known corresponding operation on integers and reducing the result modulo $N$ if necessary. We want to examine the operation of squaring and visualize the relations that are generated by repeated squaring.

This can be done by drawing a directed graph according to the following recipe:

1. Draw $N - 1$ vertices and label them $1, 2, \ldots, N - 1$.
2. Draw an arrow from every vertex to the one labeled by its square modulo $N$.
3. Arrange your picture well.

(i) As an example, the graph for $N = 19$ consists of the following three components:

![Graph for N = 19](image)

Use the information from this graph and the Repeated-Squaring-method to compute $15^{22} \text{ mod } 19$. How many multiplications are necessary?

(ii) Draw a graph for $N = 13$ and $N = 17$.

(iii) How many sources (i.e. vertices where no arrow is pointing to) does each of the graphs have.