6.2 The Arithmetic of the Base Field

For the description of AES we identify the 8-dimensional $\mathbb{F}_2$ vector space $\mathbb{F}_2^8$ and the field $\mathbb{F}_{256}$. We specify the exact mapping in the following subsections.

Algebraic Representation of the Base Field

The simplest construction of a finite field, see Appendix A, is as a factor ring of the polynomial ring $\mathbb{F}_p[X]$ over its prime field $\mathbb{F}_p$ by a principal ideal that is generated by an irreducible polynomial $h \in \mathbb{F}_p[X]$. The ideal $h\mathbb{F}_p[X]$ is prime, hence

$$K := \mathbb{F}_p[X]/h\mathbb{F}_p[X]$$

is a finite field and has degree (= dimension) $n = \deg h$ over $\mathbb{F}_p$. For the identification of K with the vector space $\mathbb{F}_p^n$ we identify the residue classes of the powers of X with the n unit vectors. So setting $x = X \bmod h$ we identify:

$$x^0 = 1 = \begin{pmatrix} 0 \\ 0 \\ \vdots \\ 0 \\ 1 \end{pmatrix}, \quad x^1 = x = \begin{pmatrix} 0 \\ 0 \\ \vdots \\ 1 \\ 0 \end{pmatrix}, \quad \ldots, \quad x^{n-1} = \begin{pmatrix} 1 \\ 0 \\ \vdots \\ 0 \\ 0 \end{pmatrix}.$$

If $h = X^n + a_1X^{n-1} + \cdots + a_{n-1}X + a_n$ (monic without loss of generality), then from $h \bmod h = 0$ we get

$$x^n = -a_1x^{n-1} - \cdots - a_{n-1}x - a_n$$

in K. Moreover this equation shows how to express the residue class of an arbitrary polynomial f by the canonical basis $1, x, \ldots, x^{n-1}$. Algorithmically this amounts to the remainder of a polynomial division "f divided by h".

For AES we use the polynomial

$$h = X^8 + X^4 + X^3 + X + 1 \in \mathbb{F}_2[X].$$

Multiplication Table

The multiplication table for the basis $(1, x, \ldots, x^{n-1})$ follows from the relation defined by h. In $\mathbb{F}_{256}$ (for AES) we have

$$x^2 \cdot x^7 = x^9 = x \cdot x^8 = x \cdot (x^4 + x^3 + x + 1) = x^5 + x^4 + x^2 + x.$$

Efficient inversion

The implementation of AES uses a complete value table of the S-box. This is efficient for we have to specify only 256 values.