General structure of AES

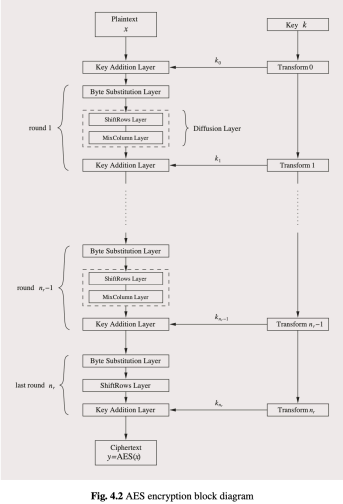

Fig. 4.2 AES encryption block diagram

From Paar, Pelzl, and Güneysu

Details of AES round structure (128 bits)

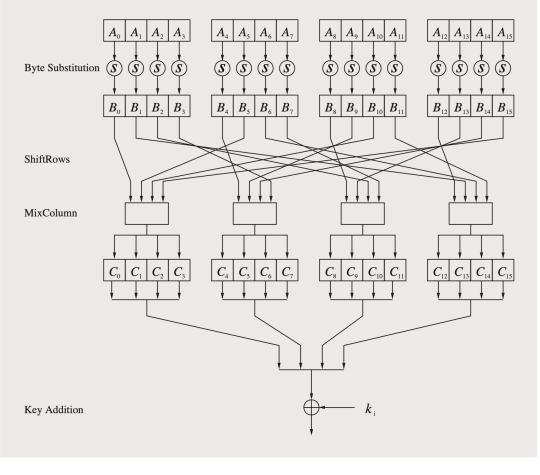

Fig. 4.3 AES round function for rounds $1, 2, \ldots, n_r - 1$

From Paar, Pelzl, and Güneysu

Perform the following calculations in $\mathbb{Z}_2[x]$

1. $(x^3 + x^2 + 1) \cdot (x + 1)$
2. $(x^3 + x + 1) \cdot (x^4 + x^2 + x)$
3. $(x^3 + x^2 + x + 1) \cdot (x + 1)$

1. Let $q(x) = x^3 + x + 1$. Perform the following calculations by hand in $\mathbb{Z}_2[x]/q(x) = GF(8)$
   (a) $(x^2 + x + 1) \cdot (x^2 + 1)$
   (b) $(x^2 + x + 1) \cdot (x + 1)$
   (c) $(x^2 + x + 1) \cdot (x^2)$
   (d) What is $(x^2 + x + 1)^{-1}$ in $\mathbb{Z}_2[x]/q(x)$?

2. Let $p(x) = x^8 + x^4 + x^3 + x + 1$. This is the polynomial specified in AES. Perform the following calculations by hand in $\mathbb{Z}_2[x]/p(x) = GF(2^8)$, recalling that we can specify any element of $GF(2^8)$ by a two-digit hex number.
   (a) $B5 \cdot 35$
   (b) $21 \cdot 31$
   (c) Verify that $C6^{-1} = E4$