Overview of AES

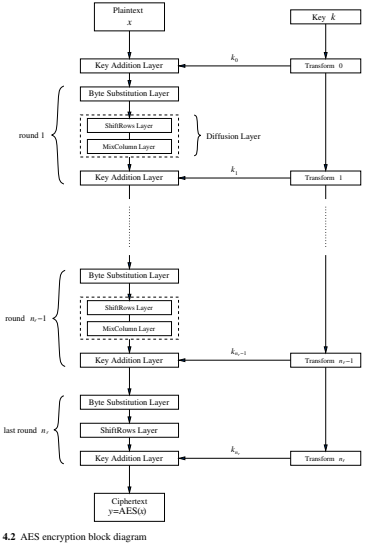

Fig. 4.2 AES encryption block diagram

Let $f(x) = x + 1$ $h(x) = x^2 + x + 1$

$g(x) = x^2 + x$ $p(x) = x^3 + x + 1$

1. Perform the following calculations in $\mathbb{Z}_2[x]$
   (a) $f(x) \cdot g(x)$
   (b) $f(x) \cdot h(x)$
   (c) $g(x) \cdot h(x)$

Let $f(x) = x + 1$ $h(x) = x^2 + x + 1$

$g(x) = x^2 + x$ $p(x) = x^3 + x + 1$

1. Perform the following calculations in $\mathbb{Z}_2[x]$
   (a) $f(x) \cdot g(x)$
   (b) $f(x) \cdot h(x)$
   (c) $g(x) \cdot h(x)$

2. Perform the following calculations in $\mathbb{Z}_2[x]/p(x)$
   (a) $f(x) \cdot g(x)$
   (b) $f(x) \cdot h(x)$
   (c) $g(x) \cdot h(x)$