Fall 2000 EE 578/CS 578 Prof. Christof Paar

Solutions to Homework Assignment # 7

1. (a) $A(x) * B(x) = (x^2 + 1)(x^3 + x^2 + 1) = x^5 + x^4 + x^2 + x^3 + x^2 + 1$
   $A(x) * B(x) = x^5 + x^4 + x^3 + 1$

$$
\begin{array}{ccccccc}
 & & & & & x & +1 \\
x^4 + x + 1 & x^5 & +x^4 & +x^3 & & & +1 \\
 & x^5 & & & +x^2 & +x & \\
 & & x^4 & +x^3 & +x^2 & +x & +1 \\
 & & x^4 & & & +x & +1 \\
 & & & x^3 & +x^2 & &
\end{array}
$$

   $C = x^3 + x^2 \equiv A(x) * B(x) \bmod P(x)$.

   (b) $A(x) * B(x) = (x^2 + 1)(x + 1) = x^3 + x + x^2 + 1$
   $C = x^3 + x^2 + x + 1 \equiv A(x) * B(x) \bmod P(x)$

2. (a) Try x: does not factor $x^3 + x^2 + x + 1$.
   Try $x + 1$:

$$
\begin{array}{ccccc}
 & & x^2 & & +1 \\
x + 1 & x^3 & +x^2 & +x & +1 \\
 & x^3 & +x^2 & & \\
 & & 0 & +x & +1 \\
 & & & x & +1 \\
 & & & & 0
\end{array}
$$

   $(x^3 + x^2 + x + 1) = (x + 1)(x^2 + 1)$.
   The polynomial is not irreducible and can not be used for constructing $GF(2^3)$.

   (b) Try x: does not factor $x^3 + x^2 + 1$.
   Try $(x + 1)$: does not factor $x^3 + x^2 + 1$.
   Try $(x^2 + x + 1)$: does not factor $x^3 + x^2 + 1$.
   Note: you do not have to try $x^2 = x * x$ and $x^2 + 1 = (x+1)(x+1)$ since those are reducible themselves and their factors have already been checked with the first two tests.
   $x^3 + x^2 + 1$ is irreducible and can be used for constructing $GF(2^3)$.

3. (a) By the Extended Euclidean algorithm:

$$\begin{array}{lll} x^4+x+1 & = [x^3](x)+[x+1] & t_2(x)=t_0-q_1t_1=-q_1=-x^3=x^3 \\ x & = [1](x+1)+1 & t_3(x)=t_1-q_2t_2=1-1*x^3=1-x^3=x^3+1 \\ x+1 & = [x+1](1)+0 & \end{array}$$

So, $A^{-1}=x^3+1$.
Check: $x*(x^3+1)=x^4+x\equiv(x+1)+x \bmod P(x)=1 \bmod P(x)$.

(b) By the Extended Euclidean algorithm:

$$\begin{array}{lll} x^4+x+1 & = [x^2+x+1](x^2+x)+[1] & t_2=t_0-q_1t_1=-q_1=x^2+x+1 \\ x^2+x & = [x^2+x]1+[0] & \end{array}$$

So, $A^{-1}=x^2+x+1$.
Check: $(x^2+x)(x^2+x+1)=x^4+2x^3+2x^2+x=x^4+x\equiv(x+1)+x \bmod P(x)=1 \bmod P(x)$.

4. (a) $d=01$, $b=1*(b_7x^7+\ldots+b_0)=b$.
$d_0=b_0$, $d_1=b_1$, $\ldots$,$d_7=b_7$.

(b) $d=02*b=x(b_7x^7+\ldots+b_0)=b_7x^8+b_6x^7+\ldots+b_0x$
$x^8\equiv x^4+x^3+x+1 \bmod P(x)$.
$d=b_6x^7+b_5x^6+b_4x^5+[b_3+b_7]x^4+[b_2+b_7]x^3+b_1x^2+[b_0+b_7]x+b_7$

$$\begin{array}{ll} d_7=b_6 & d_6=b_5 \\ d_5=b_4 & d_4=b_3+b_7 \\ d_3=b_2+b_7 & d_2=b_1 \\ d_1=b_0+b_7 & d_0=b_7 \end{array}$$

(c) $d=03*b=(x+1)b=xb+b$
Using solutions from a) and b):
$d=(b_6+b_7)x^7+(b_5+b_6)x^6+(b_4+b_5)x^5+(b_3+b_4+b_7)x^4+(b_2+b_3+b_7)x^3+(b_1+b_2)x^2+(b_0+b_1+b_7)x+(b_0+b_7)$

$$\begin{array}{ll} d_7=b_6+b_7 & d_6=b_5+b_6 \\ d_5=b_4+b_5 & d_4=b_3+b_4+b_7 \\ d_3=b_2+b_3+b_7 & d_2=b_1+b_2 \\ d_1=b_0+b_1+b_7 & d_0=b_0+b_7 \end{array}$$

5. (a) The following numbers of XOR gates are needed to do the constant multiplications in $GF(2^8)$:

Multiplication by	Number of XORs
01	0
02	3
03	$3 + 8 = 11$

(b) One matrix-vector multiplication requires the following operations in $GF(2^8)$:

8 multiplications by 01:	0	= 0 XORs
4 multiplications by 02:	$4 * 3$	= 12 XORs
4 multiplications by 03:	$4 * 11$	= 44 XORs
12 additions:	$12 * 8$	= 96 XORs
Total:		= 152 XORs

(c) The Mix Column layer requires 4 of these matrix-vector multiplications with an overall gate complexity of $4 * 152 = 608$ XORs.

6. (a) $A = 01_h$, $A(x) = 1$

$A^{-1}(x) = 1 = 01_h$

$A^{-1}(x)$ is now the input to the affine transformation of Rijndael as described in Subsection 4.2.1 of the Rijndael Specifications:

$$M \cdot A^{-1} + V$$

where M and V are a fixed matrix and vector, respectively.

$$M \cdot A^{-1} + V = M \cdot \begin{pmatrix} 1 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \end{pmatrix} + \begin{pmatrix} 1 \\ 1 \\ 0 \\ 0 \\ 0 \\ 1 \\ 1 \\ 0 \end{pmatrix} = \begin{pmatrix} 1 \\ 1 \\ 1 \\ 1 \\ 1 \\ 0 \\ 0 \\ 0 \end{pmatrix} + \begin{pmatrix} 1 \\ 1 \\ 0 \\ 0 \\ 0 \\ 1 \\ 1 \\ 0 \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \\ 1 \\ 1 \\ 1 \\ 1 \\ 1 \\ 0 \end{pmatrix}$$

ByteSub$(01_h) = 7C_h$

(b) $A = 12_h$, $A(x) = x^4 + x$

Apply extended Euclidean algorithm: $A^{-1}(x) = x^7 + x^5 + x^3 + x = AA_h$.

$$M \cdot A^{-1} + V = M \cdot \begin{pmatrix} 0 \\ 1 \\ 0 \\ 1 \\ 0 \\ 1 \\ 0 \\ 1 \end{pmatrix} + \begin{pmatrix} 1 \\ 1 \\ 0 \\ 0 \\ 0 \\ 1 \\ 1 \\ 0 \end{pmatrix} = \begin{pmatrix} 0 \\ 1 \\ 0 \\ 1 \\ 0 \\ 1 \\ 0 \\ 1 \end{pmatrix} + \begin{pmatrix} 1 \\ 1 \\ 0 \\ 0 \\ 0 \\ 1 \\ 1 \\ 0 \end{pmatrix} = \begin{pmatrix} 1 \\ 0 \\ 0 \\ 1 \\ 0 \\ 0 \\ 1 \\ 1 \end{pmatrix}$$

Remark: It is (big) coincidence that $M \cdot A^{-1} = A^{-1}$. This only holds for this specific value of A^{-1}.

ByteSub$(12_h) = C9_h$