Seminar 3

Exercise 1 (Rijndael Block Cipher Algorithm)

$A_{16} = 73_{16}$ $B_{16} = 4E_{16}$ $C_{16} = 85_{16}$ $D = (A+B)\cdot C = ?$ (in $GF(2^4)$ & $GF(2^8)$)

$A_2 = 01110011$ $B_2 = 01001110$ $C_2 = 10000101$

$x^6+x^5+x^4+x+1$ $x^6+x^3+x^2+x^1$ x^7+x^2+1

a) In $GF(2^8)$ $(\{x^8+x^4+x^3+x+1\}$ irreductible polinomial of $GF(2^8))$

$$A = x^6+x^5+x^4+x+1 \quad \oplus$$
$$B = x^6 \quad +x^3+x^2+x$$

$(A+B) = (1+1)x^6 + x^5 + x^4 + x^3 + x^2 + (1+1)x + 1$! for each %2 !

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

$(A+B)\cdot C = (x^5+x^4+x^3+x^2+1)(x^7+x^2+1) = x^{12}+x^{11}+x^{10}+x^9+x^7+x^7+x^6+$ (P(x))

~~$C = x^7+x^2+1$~~ $+x^5+x^4+x^2 + x^5+x^4+x^3+x^2+1 =$

$(A+B)\cdot C = x^{12}+x^{11}+x^{10}+x^9+(1+1)x^8+x^6+(1+1)x^5+(1+1)x^4+x^3+(1+1)x^2+1$ (P(x))

$(x^{12}+x^{11}+x^{10}+x^9+x^6+x^3+1) : (x^8+x^4+x^3+x+1) = x^4+x^3+x^2+x+1$

$x^{12}+ \quad +x^8+x^7+x^5+x^4$

$x^{11}+x^{10}+x^9+x^8+x^7+x^6+x^5+x^4+x^3+1$

$x^{11}+ \quad +x^7+x^6 \quad +x^4+x^3$

$x^{10}+x^9+x^8+x^5+1$

$x^{10}+ \quad +x^6+x^5+x^3+x^2$

$x^9+x^8+x^6+x^3+x^2+1$

$x^9 + x^5 + x^4 + x^2 + x$

$x^8 + x^6 + x^5 + x^4 + x^3 + x + 1$

$x^6 + x^4 + x^3 + x + 1$

$(A+B)C : P(x) = \boxed{x^6 + x^5}$ $\quad (A+B) \cdot C \bmod P(x) = D$

$D = x^6 + x^5$ for $GF(2^8)$

b) In $GF(2^4)$ $\quad (x^4+x+1)$ irreducible polynomial of $GF(2^4)$ as said on the following website: science-direct.com

C, B, A are not in $GF(2^4)$! We need to „reduce" them in $GF(2^4)$

$A = (x^6 + x^5 + x^4 + x + 1) : (x^4+x+1) = x^2 + x^1 + 1$

$x^6 + \quad + x^3 + x^2$

$x^5 + x^4 + x^3 + x^2 + x + 1$

$x^5 + \quad x^2 + x$

$x^4 + x^3 + 1$

$x^4 + x + 1$

$\boxed{x^3 + x}$

A in $GF(2^4)$ is $x^3 + x$

$B = (x^6 + x^3 + x^2 + \blacksquare) : (x^4 + x + 1) = x^2$

$x^6 + x^3 + x^2$

$\boxed{\blacksquare}$

B in $GF(2^4)$ is $\blacksquare$

$C = (x^7 + x^2 + 1) : (x^4 + x + 1) = x^3 + 1$

$x^7 + x^4 + x^3$

$x^4 + x^3 + x^2 + 1$

$x^4 + \quad x + 1$

$\boxed{x^3 + x^2 + x}$

C in $GF(2^4)$ is $x^3 + x^2 + x$

$A+B = (x^3+x)+(x) = x^3$ [illegible]

$(A+B)\cdot C = (x^3$ [illegible]$)\cdot(x^3+x^2+x) =$

$(A+B)\cdot C = x^6$ [illegible] $+ x^5 +$ [illegible] $+ x^4$

$(A+B)\cdot C : P(x) = (x^6+x^5+x^4) : (x^4+x+1) = x^2+x$ [illegible] $+1$

$x^6+x^3+x^2$

$x^5+x^4+x^3+x^2$

$x^5+\quad x^2+x$

[illegible]

x^4+x^3+x

$x+\quad x+1$

$\boxed{x^3+1}$

$(A+B)\cdot C : P(x) = \boxed{x^3+1}$ in $GF(2^4)$