Seminar 3

1) $A = 73_{16}$ $B = 4E_{16}$

$C = 85_{16}$

$D = (A+B) \cdot C$

For $GF(2^8)$

$m_8(x) = x^8 + x^4 + x^3 + x + 1$

For $GF(2^4)$

$m_4(x) = x^4 + x + 1$

Step 1: Compute $A+B$ in $GF(2^m)$

$A = 73_{16} = 01110011_2$

$B = 4E_{16} = 0100\ 1110_2$

$A+B$ in $GF(2^m) \Leftrightarrow A \oplus B$

$$\begin{array}{r} 01110011 \ \oplus \\ 01001110 \\ \hline 00111101 \end{array} = 3D_{16}$$

$A+B = 3D_{16}$

Step 2A: Compute $D = (A+B) \cdot C$ in $GF(2^8)$

Interpret the elements as Polynomials

$A+B = 3D_{16} = 00111101_2$

$\to (3D)(x) = x^5 + x^4 + x^3 + x^2 + 1$

$C = 85_{16} = 1000\ 0101_2$

$\to (85)(x) = x^7 + x^2 + 1$

Multiply the polynomials

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

$G(x) = (x^7 + x^2 + 1)$

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

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

Reduce $P(x)$ modulo $m_8(x)$

1. Divide x^{12} by x^8

Quotient term $= x^4$

Multiply: $x^4 \cdot m_8(x) = x^{12} + x^8 + x^7 + x^5 + x^4$

~~xor~~ with $R(x)$:

$R(x) \oplus (x^{12} + x^8 + x^7 + x^5 + x^4)$

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

2. Divide the new leading term x^{11} by x^8

$Q = x^3$

multiply $x^3 \cdot m_8(x) = x^{11} + x^7 + x^6 + x^4 + x^3$

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

3. Divide x^{10} by x^8

$Q = x^2$

$x^2 \cdot m_8(x) = x^{10} + x^6 + x^5 + x^3 + x^2$

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

4. Divide x^9 by x^8

$G = x$

$x \cdot m_8 = x^9 + x^5 + x^4 + x^2 + x$

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

5. Divide x^8 by x^8

$6 = 1$

$m_8(x) = x^8 + x^4 + x^3 + x + 1$

XOR: $x^6 + x^5$

Step 2B: Compute $D = (A+B) \cdot C$ in $GF(2^4)$

Reduce A, B and C modulo $m_4(x)$

$m_4(x) = x^4 + x + 1$

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

1. $Q = x^2$

   $x^2(x^4 + x + 1) = x^6 + x^3 + x^2$

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

2. $Q = x$

   $x(x^4 + x + 1) = x^5 + x^2 + x)$

   XOR: $x^4 + x^3 + 1$

3. $Q = 1$

   $x^4 + x + 1$

   XOR: $x^3 + x$

$A' = 1010_2 = A_{16}$

$B(x) = x^6 + x^3 + x^2 + x$

1. $Q = x^2$

   $x^2(x^4 + x + 1) = x^6 + x^3 + x^2$

   XOR: x

$B' = 0010_2 = 2_{16}$

$C(x) = x^7 + x^2 + 1$

1. $Q = x^3$

   $x^3(x^4 + x + 1) = x^7 + x^4 + x^3$

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

2. $Q = 1$

   $x^4 + x + 1$

   XOR: $x^3 + x^2 + x$

   $C' = 1110_2 = E_{16}$

$A' + B' = \quad 1010 \oplus 0010 = 1000_2 = 8_{16}$

$D' = (A' + B') \cdot C' = (x^3 + x^2 + x) \cdot x^3 = x^6 + x^5 + x^4$

1. $Q = x^2$

   $x^2(x^4 + x + 1) = x^6 + x^3 + x^2$

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

2. $Q = x$

   $x(x^4 + x + 1) = x^5 + x^2 + x$

   XOR: $x^4 + x^3 + x$

3. $Q = 1$

   $x^4 + x + 1$

   XOR: $x^3 + 1$

$D = 1001_2 = 9_{16}$