Seminar 3

1. Rijndael Block Cipher

$A = (73)_{16} = (\underset{x^7}{0}\underset{x^6}{1}\underset{x^5}{1}\underset{x^4}{1}\ \underset{x^3}{0}\underset{x^2}{0}\underset{x}{1}\underset{x^0}{1})_2 \quad = x^6 + x^5 + x^4 + x^1 + 1$

$B = (4E)_{16} = (0100\ 1110)_2 \quad = x^6 + x^3 + x^2 + x$

$C = (85)_{16} = (1000\ 0101)_2 = x^7 + x^2 + 1$

$A + B = (x^6 + x^5 + x^4 + x + 1) + (x^6 + x^3 + x^2 + x) = x^5 + x^4 + x^3 + x^2 + 1$

~~$(A+B) \cdot C = (x^5 + x^4 + x^3 + x^2 + 1)(x^6 + x^3 + x^2 + x)$~~ $(x^7 + x^2 + 1)$

~~$= x^{12} + x^7 + x^5 + x^{11} +$~~

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

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

$GF(2^8)$: $(A+B) \cdot C \mod (x^8 + x^4 + x^3 + x + 1)$

$$\begin{array}{l|l}
x^{12} + x^{11} + x^{10} + x^9 + x^6 + x^3 + 1 & x^8 + x^4 + x^3 + x + 1 \\ \cline{2-2}
x^{12} + x^8 + x^7 + x^5 + x^4 & x^4 + x^3 + x^2 + x + 1 \\ \hline
/ + x^{11} + x^{10} + x^9 + x^8 + \cancel{x^7} + \cancel{x^6} + x^5 + x^4 + \cancel{x^3} + 1 & \\
x^{11} + \cancel{x^7} + \cancel{x^6} + \cancel{x^4} + \cancel{x^3} & \\ \hline
\cancel{x^{10}} + x^9 + x^8 + \cancel{x^5} + 1 & \\
\cancel{x^{10}} + x^6 + \cancel{x^5} + x^3 + x^2 & \\ \hline
x^9 + x^8 + x^6 + x^3 + \cancel{x^2} + 1 & \\
x^9 + x^5 + x^4 + x^2 + x & \\ \hline
x^8 + x^6 + x^5 + x^4 + x^3 + \cancel{x} + 1 & \\
x^8 + x^4 + x^3 + x + 1 & \\ \hline
x^6 + x^5 &
\end{array}$$