2WC12 Cryptography I - Fall 2009
Homework 25.09.2009

1) Problem B.7 in Appendix B

2) Problem B.8 in Appendix B

3) AES. In the function `MixColumns` of the AES algorithm, a vector r is given by $r = Tc$ with $c = (c_0, c_1, c_2, c_3)^T$, $c_i \in \mathbb{F}_{2^8}[x]$, and

$$T = \begin{pmatrix} x & (x+1) & 1 & 1 \\ 1 & x & (x+1) & 1 \\ 1 & 1 & x & (x+1) \\ (x+1) & 1 & 1 & x \end{pmatrix}.$$

Show that

$$(c_3u^3+c_2u^2+c_1u+c_0)((x+1)u^3+u^2+u+x) = r_3u^3+r_2u^2+r_1u+r_0 \mod u^4+1.$$