CMSC 652
Spring 2006
Homework 4

Due: Wednesday, March 8, 2006

Reading Assignment:

- Douglas R. Stinson, "Cryptography: Theory and Practice," (Third edition), Chapman & Hall/CRC, (2006). Read chapters 2
- Peterson, W. Wesley, "Error-Correcting Codes, MIT Press, (1961). Read Chapter 2 (The class handout)

Homework:

1) The polynomial $p(x) = x^2 + x + 2$ is primitive (hence, irreducible) over $GF(3)$. Use $p(x)$ to construct a log/antilog table for $GF\left(3^2\right)$.

2) (a) Draw the linear sequential circuit (LSC) that multiplies by the polynomial
$$h(x) = 1 + x^3 + x^6$$
(b) Draw the linear sequential circuit (LSC) that divides by the polynomial
$$g(x) = 1 + x^2 + x^4 + x^6 + x^7$$
(c) Draw the linear sequential circuit (LSC) that simultaneously multiplies by $h(x)$ and divides by $g(x)$.

3) Draw an LSC which takes as inputs polynomials $a(x)$ and $b(x)$, and then produces the output $h(x)a(x) + k(x)b(x)$, where $h(x)$ and $k(x)$ are the polynomials:
$$h(x) = 1 + x^4 + x^{10} \text{ and } k(x) = x + x^2 + x^4 + x^7 + x^9$$