CMSC 652
Spring 2006
Homework 2

Due: Wednesday, February 22, 2006

Reading Assignment:

- Douglas R. Stinson, "Cryptography: Theory and Practice," (Third edition), Chapman & Hall/CRC, (2006). Read chapter 1.

Homework:

1) Use the extended Euclidean algorithm to compute $d = \gcd(899, 493)$ and integers a and b such that $d = a \bullet 899 + b \bullet 493$.

2) Given polynomials

$$a = x^{12} + x^7 + x^2 + x + 1 \bmod 2$$

and

$$b = x^{14} + x^{13} + x^{10} + x^9 + x^8 + x^7 + x^5 + x^3 + 1 \bmod 2,$$

lying in the ring $\mathbb{Z}_2[x]$, use the Euclidean algorithm to find $\gcd(a,b)$.

3) Exercise 1.24 on page 42 of the text.