CMSC 652
Spring 2006
Homework 3

Due: Wednesday, March 1, 2006

Reading Assignment:

- Douglas R. Stinson, "Cryptography: Theory and Practice," (Third edition), Chapman & Hall/CRC, (2006). Read chapters 1 and 2
- Dorothy Denning, "Cryptography and Data Security," Addison-Wesley, (1982). Read chapter 2.

Homework:

1) Construct a multiplication table of the group given by the presentation

$$\left(r, s : r^4 = s^2 = 1, sr = r^3 s\right)$$

You may assume that the distinct elements of this group are

$$1, r, r^2, r^3, s, rs, r^2 s, r^3 s$$

2) The polynomial $p(x) = x^5 + x^3 + 1$ is primitive (hence, irreducible) over $GF(2)$. Use $p(x)$ to construct a log/antilog table for $GF\left(2^5\right)$.