Cryptology
Problems

To be discussed Monday, April 10, 2000.

1. Do problems 5.7, 8.3, and 8.5 in the textbook.

2. Suppose $p \equiv q \equiv 3 \pmod 4$ are both primes and $n = p \cdot q$. Suppose x is a QNR modulo both p and q. Show that $-x$ is a QR modulo n.