

CMSC 652

Spring 2006

Homework 6

Due: Wednesday, April 26, 2006

Reading Assignment:

- Douglas R. Stinson, "Cryptography: Theory and Practice," (Third edition), Chapman & Hall/CRC, (2006). Read chapter 5

Homework:

1) Use Garner's algorithm (using the positive representation, and then again using the symmetric representation) to find the unique integer u in the range $0 \leq u < 315$ such that

$$\begin{cases} u = 2 \pmod{5} \\ u = 4 \pmod{7} \\ u = 8 \pmod{9} \end{cases}$$

2) Use the extended algorithm (as explained in class) to find the $d = \gcd(3801, 525)$ and integers s and t such that $d = s(3801) + t(525)$.

3) Exercise 3.5, page 114

4) Exercise 3.6, page 115