

MAT 312/AMS 351 – Fall 2010
Homework 8

1. In p. 56 problem (6), check that the first block (13615) decodes to 40 = “O”. You may do this as follows: first check that the multiplicative inverse of 121 modulo $\varphi(23711) = 23400$ is 3481. Show your work. Then use a calculator to compute 13615^{3481} modulo 23711 by calculating the following powers of $13615 \pmod{23711}$: 2, 4, 8, 10, 20, 40, 80, 100, 200, 400, 800, 1000, 2000, 3000, 3400, 3480, 3481.
2. Decode the second block (19917). Show your work!
3. page 76 problem (1).
4. page 76 problem (2).
5. A transposition is a cycle of length 2. Check the (elementary) proof on p. 82 that every cycle is a product of transpositions. Then prove that every permutation is a product of transpositions.
6. Explain why that product is not unique.
7. Write the permutation

$$\pi = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 4 & 6 & 1 & 8 & 7 & 5 & 2 & 3 \end{pmatrix}$$

as a product of transpositions.