University of Limerick
Dr. Bernd Kreussler

1 October 2015
Exercise Sheet 4

MA 6011 (Cryptographic Mathematics)

Solve Problems 1–4 ***before*** *the tutorial on Tuesday, 6 October.*

Problem 1: Use successive squaring to find the following:

(i) $7^{32} \mod 101$

(ii) $7^{41} \mod 101$

(iii) $7^{152} \mod 101$

Problem 2: Find the smallest positive integer n such that

(i) $n^{17} \equiv 10 \mod 29$

(ii) $n^{23} \equiv 7 \mod 68$

(iii) $n^{123} \equiv 7 \mod 345$

Problem 3: Find the private key d when the public key consists of the pair

$$m = 377 \quad \text{and} \quad k = 139.$$

Problem 4: Verify the following result for the cases $n = 2, 3, 4, \dots, 10$.

Wilson's Theorem: An integer n is prime if and only if

$$(n-1)! \equiv -1 \mod n.$$

Can this be used as an efficient test for a number to be prime?

Implement the following in sage ***before*** *we meet for the lab on Tuesday, 13 October.*

Problem 5: Programme Rowland's formula and verify his results. Try different starting values and see what happens.

Problem 6: Write a sage function that takes two positive integers L, S as input. It should return the list of integers $a_0, a_1, \dots, a_k$ that is obtained by breaking up S into blocks of length L (starting at the right end).
For example, if $L = 3$ and $S = 1234567890$ the function should return the list with elements $a_0 = 1, a_1 = 234, a_2 = 567, a_3 = 890$.