Cryptography 1, Homework 12

Mark Vijfvinkel & Aram Verstegen
0863002(s134674), 100863(s4092368)
Radboud University

December 18, 2013

1 Question 1 & 2:

Sage has a very nice function named: euler_phi(n).
We used this to calculate question 1 and 2, the results are shown below:
Question 1: 8640
Question 2: 379247933987370471260160

2 Question 3:

The public key (e, n): (23441, $p \cdot q$) = (23441, 103487)
The private key (n, d): (103487, $d \equiv e^{-1} \pmod{\phi(n)}$) = (103487, $d \equiv 23441^{-1} \pmod{\phi(103487)}$) = (103487, $d \equiv 23441^{-1} \pmod{102816}$) = (103487, 67889)

3 Question 4:

4 Question 5:

We have the following congruences:
$x \equiv 0 \pmod 3$
$x \equiv 1 \pmod 5$
$x \equiv 2 \pmod 8$

We can transform them in the following system of equations:
$x = 0 + 3t$
$x = 1 + 5u$
$x = 2 + 8v$

We plug the first equation into the second congruence:
$0 + 3t \equiv 1 \pmod 5$
$3t \equiv 1 \pmod 5$
$t \equiv \frac{1}{3} \pmod 5$
$t \equiv 2 \pmod 5$
$t = 2 + 5u$

We can plug this into the first equation:
$x = 0 + 3t = 0 + 3 \cdot (2 + 5u) = 6 + 15u$

This we can plug into the third congruence:
$6 + 15u \equiv 2 \pmod 8$
$15u \equiv -4 \pmod 8$
$u \equiv \frac{-4}{15} \pmod 8$
$u \equiv 4 \pmod 8$

$u = 4 + 8v$

We can plug this into the equation above:

$$6 + 15 \cdot 4 + 8v = 6 + 60 \cdot 120v = 66 + 120v$$

So the smallest positive integer to satisfy the system of congruences is 66. The following values would be 66 plus a multiple of a 120.