Math 3 (V3020) — Exercises, week 4

1. Decrypt the unknown shift cipher message that is known to be in English.

ZAHYA CVYRPUN VU AOL OVTL
LDHT WYVQLJA

Since we know that the message is in English that has 26 letters in its alphabet, we could crack the code with brute force by trying the inverse shift function $f^{-1}(n) = (n-k) \bmod 26$ for every $k = 0, 1, \ldots, 25$, where n is the label of a letter $A=0$, $B=1$, $\ldots$, $Z=25$.

A more clever way is to use the structure of the English language to our advantage. The message has a two letter word followed by a three letter word VU AOL. The most common two letter words are prepositions and "the", "and", "are" are the most common three letter words.

Our best guess would be thus that VU AOL stands for "IN THE", "ON THE", "OF THE" etc.

To transform "AOL" (0 14 11) to "THE" (19 7 4), we use $f^{-1}(n) = (n-7) \bmod 26$.

We see that this made sense, since after this transformation, the message reads START WORKING ON THE HOME EXAM PROJECT

2. Decrypt the message
25151440 13535569 4998754.

You know the public keys $k = 86123123$ and $m = 94642061$. You're the one who generated the keys, so you also know the two primes $p_1 = 10093$ and $p_2 = 9377$ so that $m = p_1 p_2$.

Because you know m's prime decomposition, you can calculate Euler's ϕ function at m:

$$\phi(m) = \prod_{p|m} \left(p^{\alpha(p)} - p^{\alpha(p)-1} \right) = (p_1 - 1)(p_2 - 1)$$
$$= 94\,622\,592$$

and with the Euclidean algorith, you can check $(\phi(m), k) = 1$.

m is quite small, so we assume the message to be encrypted in blocks. So we denote
$b_1 = 25151440$, $b_2 = 13535569$, $b_3 = 4998754$

For the decryption protocol, we want to find k' such that $k'k \equiv 1 \bmod \phi(m)$

The extended Euclidean algorithm is used to find k' and q that solve
$k'k + q\phi(m) = 1$
and we find $k' = -13\,862\,341$ and $q = 12617157$.

This is a solution, but we require a solution with a positive k'. Given that k' and q are solutions and $(k, \phi(m)) = 1$ divides 1, the general solutions are of the form
$k'_0 = k' + w\,\phi(m)/(k, \phi(m))$
$q_0 = q - w\,k/(k, \phi(m))$
for some $w \in \mathbb{Z}$.

We use $w = 1$ to get the smallest positive solution and call it $k'' = k' + \phi(m) = 80760251$
($q'' = q - k$ and you can check that $k''k + q''\phi(m) = 1$ is correct.)

We then need to find numbers c_j, $j = 1, 2, 3$, that satisfy $c_j \equiv b_j^{k''} \bmod m$.

These numbers are easily found using a fast modular exponentiation algorithm

$c_1 = 072\ 101$

$c_2 = 108\ 108$

$c_3 = 111\ 033$

An extra 0 is added to the front of c_1 to format it to three number blocks. This is done because we know the original message was encoded from the decimal representation of the ASCII characters. Our c_j then give the original message, as $072 = H$, $101 = e$, $108 = l$, $111 = o$, $033 = !$

The message can be read "Hello!"