ASSIGNMENT 3 RSA

Thom Scholtens 500766849 & Vincent Hoogstra 500756820
T.scholtens@hva.nl & V.hoogstra@hva.nl

Table of contents

Encryption

Step 1

Explanation

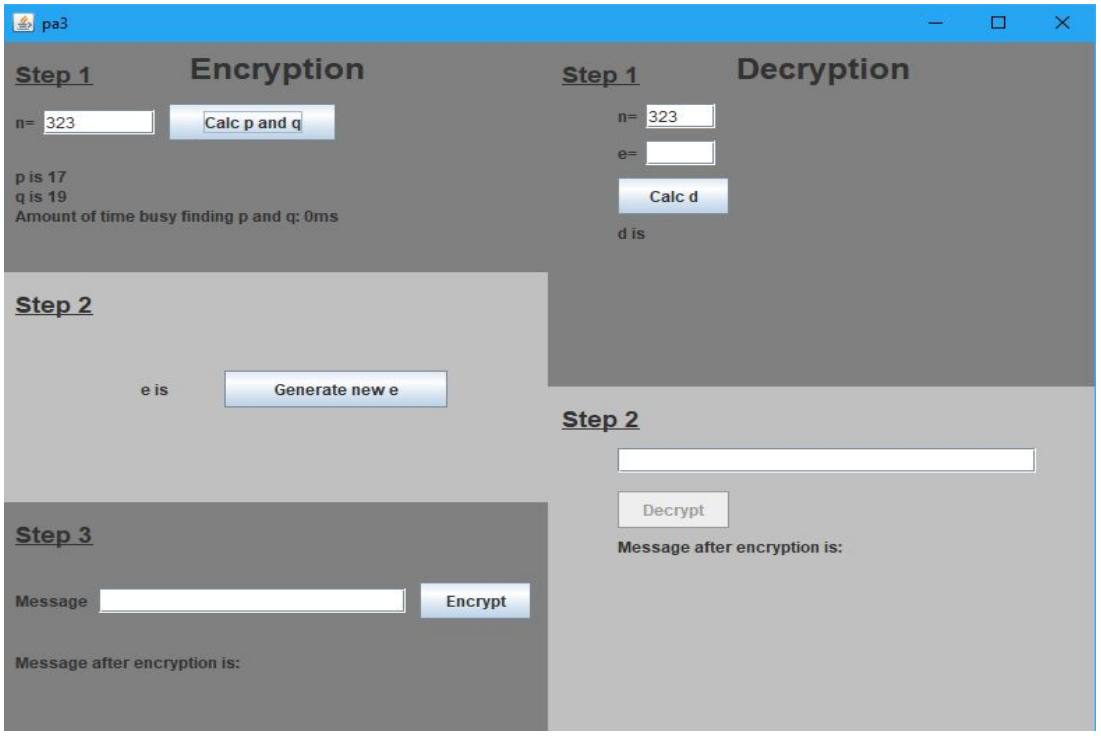
The first step is to fill in a number n. The program then calculates p and q which are two prime numbers that are equal to n when they are multiplied by each other. So: n = pq, where p and q are prime numbers.

The algorithm to calculate p and q works like this:
We first get the smallest prime number, which is 2, for p.
Secondly we get the smallest prime number for q, this is also 2.

We now check if n/q equals p and is not a decimal number.
If this is not true we increase q to the next prime number until it's not smaller then n anymore.
If the next prime number is bigger then n we reset q to 2 and increase p to the next prime number.
If n/q is smaller then q we also increase p and reset q for efficiency.

Result

Fill in n like the example below, the program will calculate p and q when you press the button. N should be a number that is the result of 2 prime numbers multiplied. We haven't implemented big numbers, so n should be a valid int value. For ease of use we also copy the n to step 1 of decrypt.



Step 2

Explanation

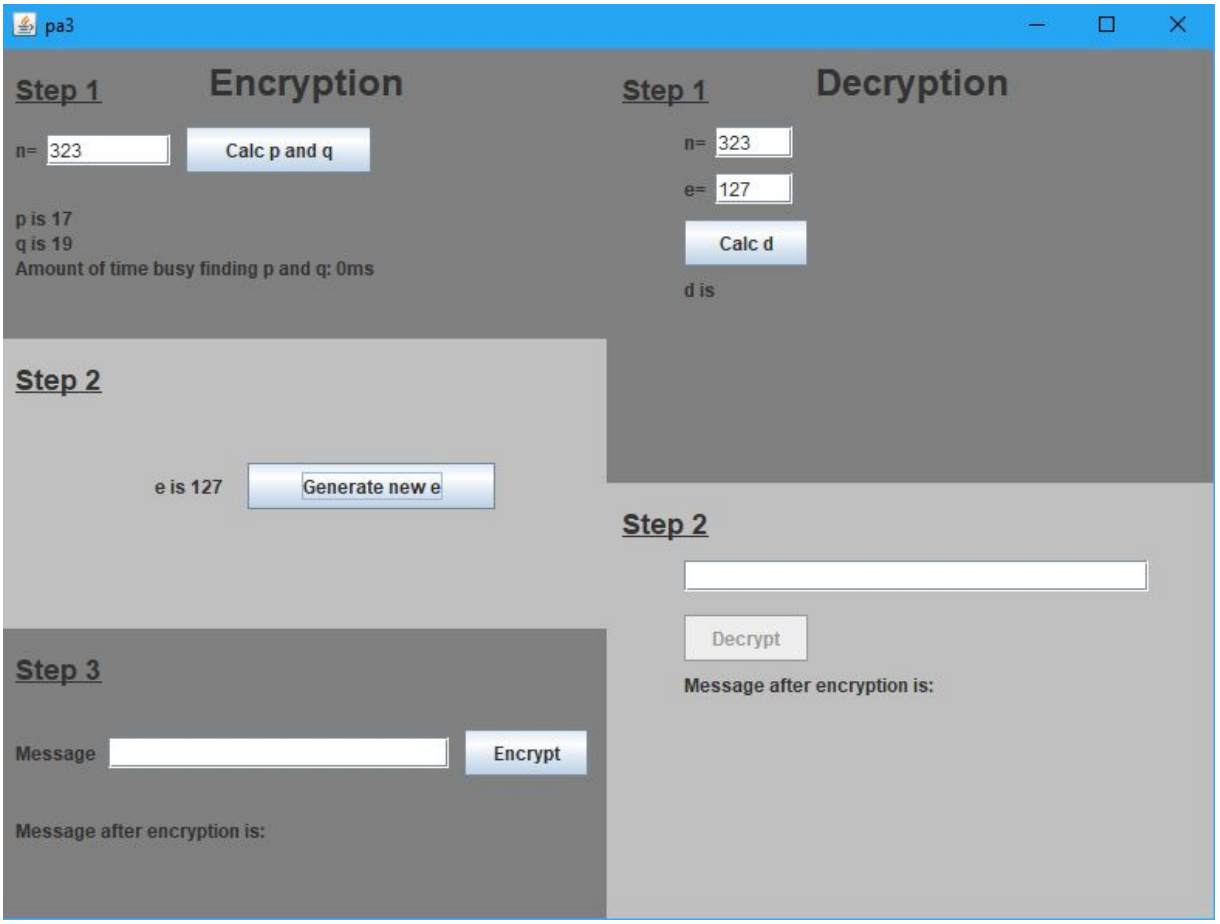
Step 2 is to calculate e. To do this we first need to calculate phi:

$$phi = (p-1)(q-1)$$

Now we can calculate e which is a number between 1 and phi, is prime and the greatest common divider between e and phi is 1. So we generate a random number, until those conditions are true, and that number is e.

Result

Once p and q are calculated you can press the button on step 2. This will calculate or recalculate the e. this is also prefilled in step 1 of the decrypt for ease of use.



Step 3

Explanation

We start by converting the string to an Integer list. We do this through unicode.

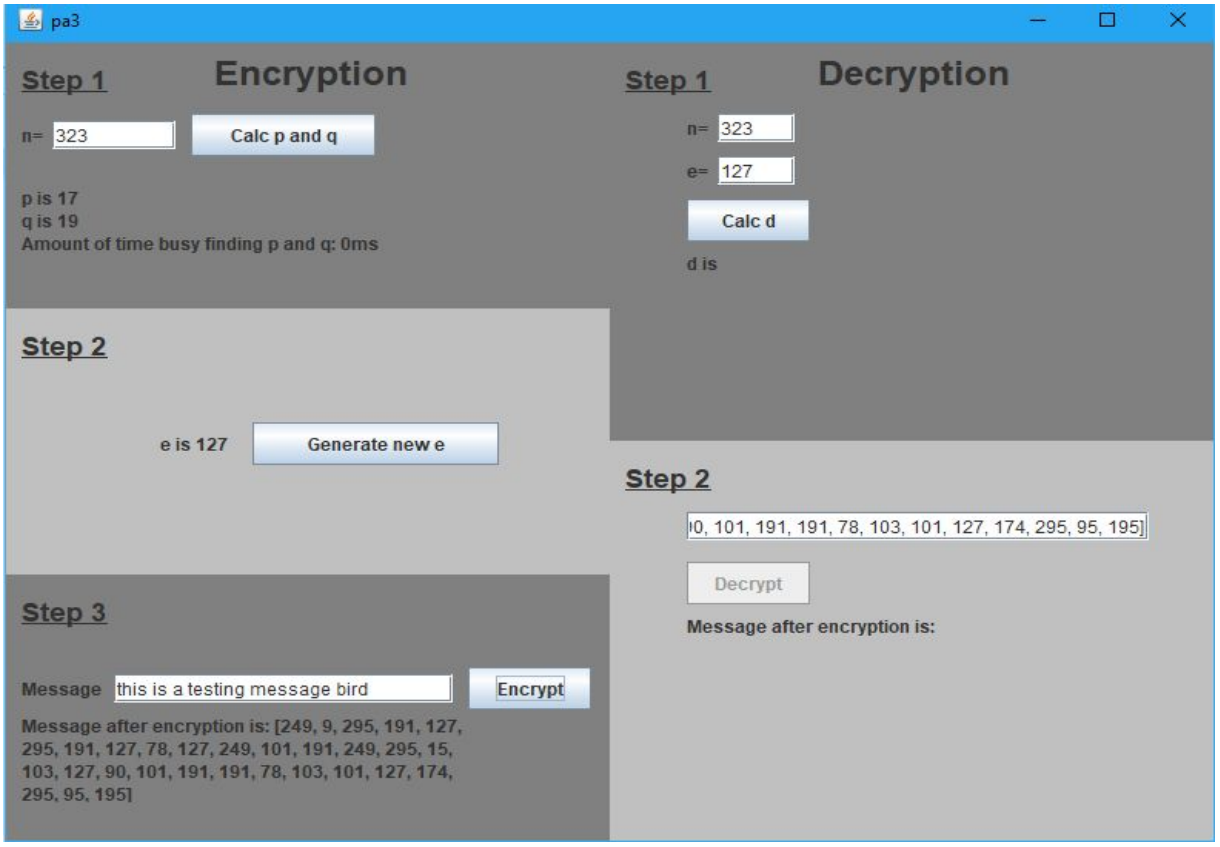
Next we walk over this list and do the item power of e. the result of this we do modulo n which gives us the encrypted number. So we use the following formula:

$$c^e \% n$$

Where:
c is the list item
we generated e in step 2
n was given in step 1.
We put those encrypted values into an array, which is the encrypted message.

Result

This step will encrypt the message. So fill in a message in the field and press the encrypt button. The decrypted message will be shown on the screen and automatically filled in in the textfield in step 2 of decryption for ease of use



Decryption

Step 1

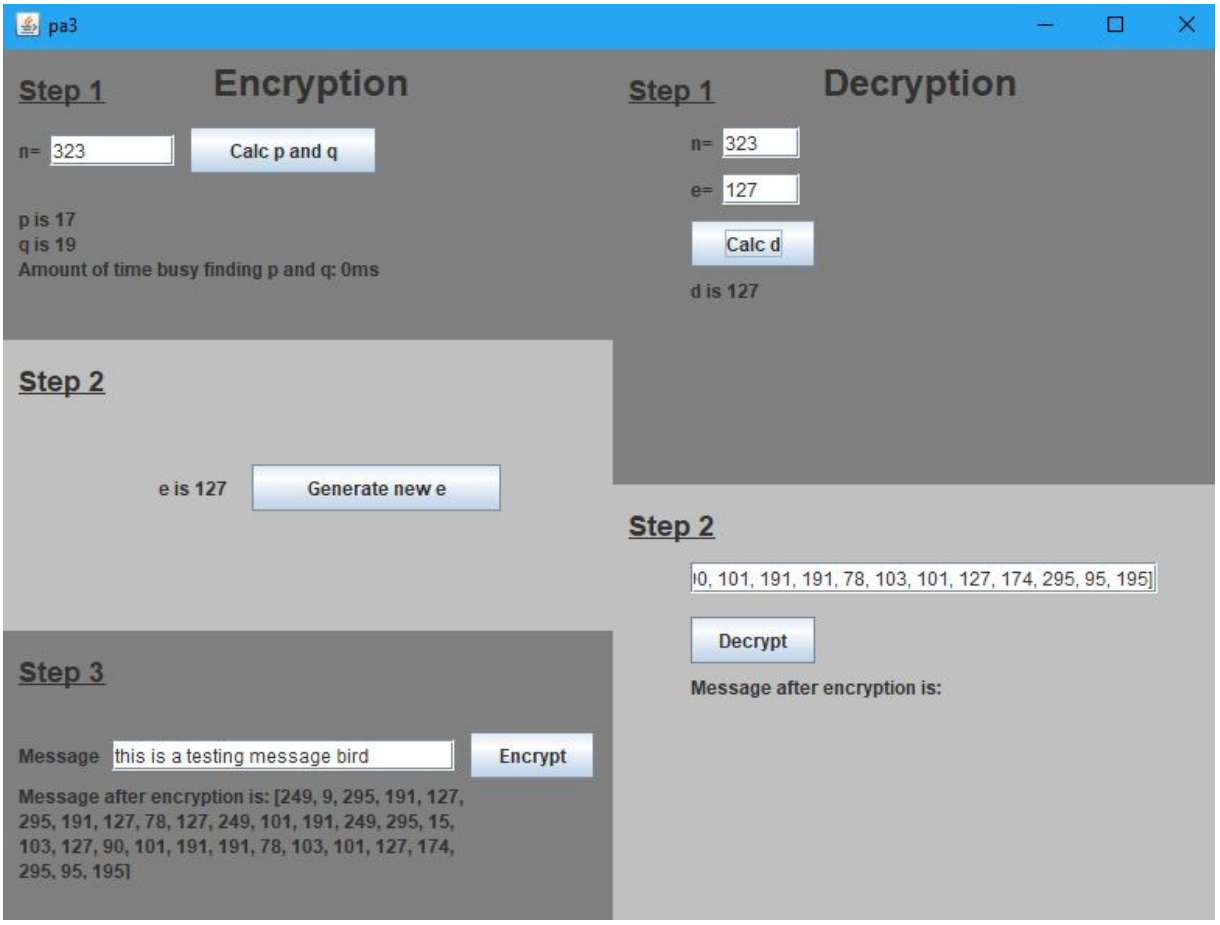
Explanation

We ask for N and E. we then again calculate p, q and phi as stated above.
after we get those we calculate d, which is done by the following formula:

$$(e^{-1} \ \% \ phi)$$

Result

after the n and e are filled in we calculate the d. n and e may be already filled if the encryption is done first. If you want to test with a different e value you can manually change e and recalculate d. You will see the decryption in step 2 will fail.



Step 2

Explanation

First we translate the string we get from the input into an Integer arraylist.
then we walk over this array with the following formula.

$$c^d \% n$$

Where:
c is the list item
we generated d in step 1
n was given in step 1.

then we put the arraylist in a stringbuilder to create a normal output. This will be the decrypted text

Result

Fill in the arraylist. if encryption is done first it is prefilled. the array can be given with the [ ] around it or without it. once the decrypt button is pressed the system will translate it.