

Successive Powers (60pts)

You have an input which takes a number multiples it by a certain number and then throws away everything except the remainder after dividing it by some number

The list is as follows:

{588, 665, 216, 113, 642, 4, 836, 114, 851, 492, 819, 237}

We want to find the the secret prime number (p) and the secret multiplier (x)

The machine always does the following

Next_no. = (now_number * x) mod p

We have two successive numbers (113, 114)

Lets see how they work

$$113 * x = 642 \pmod{p}$$

$$114 * x = 851 \pmod{p}$$

This can also be written as, $114x - 113x = 851 - 642 \pmod{p}$

Forget about mod p for the moment

$$X = 209 \pmod{p}$$

Now insert that into any equation well use the one from above

$$113 * 209 = 642 \pmod{p}$$

$$23,617 = 642 \pmod{p}$$

$$23617 - 642 = \pmod{p}$$

$$22975 = \pmod{p}$$

Now find its factors to find p

4595, 5, 919 – the only three number factor is 919 so p is 919