

## GROUP WORK, WEDNESDAY AFTERNOON

*There is no castle so strong that it cannot be overthrown by money. – Cicero*

We fix a prime modulus  $p$ . The security of one of the main modern cryptographic protocols is based on the following problem. Solving the equation

$$x^? \equiv_p b$$

for  $?$  is *HARD*. It takes a long time. We will explore using the computer to see how hard it is.

First we do the following however.

1. We find a generator for the following table of primes. (Remember a generator is a number  $x$  such that every number between 1 and  $p-1$  is a power of it modulo  $p$ ). You can use the computer to help with finding a generator (you can ask it whether a given number is a generator, use the guess and check method).

Prime	Generator
37	
41	
103	
557	
6971	
27823	
854527	
4763959	
864308560711	
583705352761272481	

**2.** Fill in the table below using the information from the previous page. We are going to use  $x$  as your generator and we are going to solve the following equations

$$x^? \equiv_p b$$

for ? Do the first one by hand (ie, find what power you need to raise  $x$  to to get  $b = 7$ ). Verify that the solutions the computer finds are correct and try to time the computer with a stopwatch or on a smartphone/computer/watch.

Prime	Generator = x	b	exponent/?	Time
37		7		
41		32		
103		55		
557		224		
6971		1111		
27823		23189		
854527		161243		
4763959		1234567		
864308560711		134308560721		
583705352761272481		283705352765273486		