Project 3 – Writeup

Tony Potter

GTID 90xxxxxxxx

In Task 2, we had to find the private key, given a public key. I used a quick way to get primes knowing that all primes other than 2, 3, and 5 (which are easy to check for) are congruent modulo 30 to an element of {1, 7, 11, 13, 17, 19, 23, 29}. Using this, I can iterate through a smaller number of values to directly test by division. I also start at the square root of n, under the assumption that the primes will be equally large in magnitude and relatively close together. Starting at a prime just over the square root of n and working backwards through the list of primes discussed earlier, I was able to determine the two prime factors of n rather quickly. Once I found these two primes, it was simply a matter of calculations to find appropriate d given e (although it’s quite nice that the gcd function in python has a three-parameter prototype that automatically performs the modular arithmetic.)

In Task 3, due to an issue with the random number generator, a common prime was used to determine my n1 and another’s n2. Thus, if p divides n1 and n2, then gcd(n1,n2) is at least p. I found the gcd, and used that p to find my q and my totient ɸ(n). Using the same three-parameter gcd function I used in Task 2, I found my private key.