Jacob Kilver

Introduction to Information Security

Assignment 3

20 Nov 2016

# Task 2 – Attack Small Key Space

## Find p and q

To factor the public key N I used the algorithm based on the one outlined here: <http://www2.mae.ufl.edu/~uhk/FACTORING-LARGE-COMPOSITE-NUMBERS.pdf>. We know that N is the product of primes p and q:

We also know that the sum of two prime numbers is an even number. We can represent the sum of p and q as follows:

Where n is the average integer value of p and q. We eliminate q from the equations to solve for p

Substituting p, we can solve for q:

To search for p and q, I iterated through different values of n. I started at the square root of N and worked my way up. Once I found an integer value for p using the equation above, I solved for q and exited. This seemed to efficiently find the values for p and q.

## Find private key

From lecture and the textbook, we know that the private key must satisfy the following equation:

where φ(N) is the totient of public key N. I interpreted this equation to be the following equivalent statement:

where k is any positive integer. Integer k handles the fact that the modulo operator repeats. This formulation allowed me to search the private key space much more efficiently since I only had to search values of k until the k equaled e. For some reason that I am still exploring, the equation above did not yield a valid d for every value of k. I had to explicitly check if the value of d satisfied the identity in the first equation. If it did, I found the private key, and so I exited the loop.

# Task 3 – Where is Waldo?