MATH 356 Number Theory
Python Worksheet 4: RSA

Use Python to try out RSA by following the steps below. You may want to have your code for φ, and remember to `import math`.

1. Encode and decode a simple numerical message.

   (a) Let $p = 43, q = 47$, and let $n = pq$.

   (b) Let $m = \varphi(n)$.

   (c) Choose an encoding key e such that $\gcd(e, m) = 1$.

   (d) Encode the message "42" using RSA: find $42^e \mod n$.

   (e) Now find your decoding key d.

   (f) Decode your message M using d: find $M^d \mod n$. Is it your original message, 42?

2. Now set up your own RSA system in teams.

   (a) Choose your own three- to four-digit primes p and q and compute $n = pq$.

   (b) Let $m = \varphi(n)$.

   (c) Choose an encoding key e such that $\gcd(e, m) = 1$ and find your decoding key d.

   (d) Encode a numerical message $M < n$ (with $\gcd(M, n) = 1$) using RSA: find $M^e \mod n$.

   (e) On the board, write your n, your e, and your message $M^e \mod n$.

   (f) First team to decode all messages gets Red Vines! (So does everyone else, but they'll have to wait.)