JUNE 21ST CRYPTOGRAPHY PROBLEM SET

A cure? A cure! Do you have any idea how easy it will be for me to make a new virus? All I have to do is find a very large prime number and multiply. – Bob Page.

RSA is secure because it is hard to factor large numbers. Especially numbers $m = pq$ where p and q are prime. However, if you choose your primes poorly, the factorization is actually quite fast. We will learn one such way to factor large numbers now. We start with the algorithm.

(i) Pick a small number $a_1 = a > 1$.
(ii) Compute $\gcd(a, m)$. If > 1 we found a factor of m and we are done.
(iii) Start a loop with $i \geq 1$ increasing at each step. In Sage, this should probably be a `while` loop.
  (iii.a) Define $a_i = a_{i-1}^i \pmod{m}$.
  (iii.b) If $a_i = 1$, go back to (i) and choose a new a.
  (iii.c) Compute $d = \gcd(a_i - 1, m)$, if > 1 exit the loop.
(iv) If $d \geq m$, go back to (i) and choose a new a. Otherwise, d is a nontrivial factor of n and we are done.

This is a good way to find factors if p (or q) has the property that $p - 1$ has lots of small factors. Indeed, this method should work if $p - 1$ divides $k!$ evenly (written $(p-1) \mid k!$) where you are willing to do k steps (like if k is a billion, a computer can do it).

Let's do an example.

1. Use the above method to factor 299 starting with $a = 2$.

2. Now do a harder example. $m = 3193$.

3. And even harder, $m = 30227$.

4. See if you can figure out why this process should always stop when $i = k$ and $(p-1) \mid k!$.

Hint: Explain why $a_i = a^{i!} (\text{mod } m)$. Consider $a_k (\text{mod } p)$ using the fancy Fermat's little theorem. What is $a_k - 1 (\text{mod } p)$? Use this to show that $\gcd(a_k - 1, n) > 1$.