FACTORING THE SEMI-PRIME N=1122973

We show how to factor large semi-primes using some new properties found by us during the last decade and discussed at length on this TECH-BLOG page. Starting with the important new fact that any semi-prime N=pq and its components must have the form –

$$N=6k\pm1, \qquad p=6n\pm1, \qquad \text{and} \qquad q=6m\pm1$$

provided all numbers N, p, and q are five or greater'

The sign in ± is chosen to be consistent with the N expansion. To demonstrate our factoring approach we confine our attention in this article to the seven digit long semi-prime-

$$N=1122973=6(187162)+1$$

The plus sign follows from noting that N mod(6)=1. A minus sign in N would mean N mod(6)=5. The prime components (from two possibilities) here can be written as-

$$p=6n-1 \quad \text{and} \quad q=6m-1$$

Substituting into N, produces the equation-

$$6nm-(n+m)=(N-1)/6=187162$$

Solving for m produces-

$$\mathbf{m=(187162+n)/(6n-1)}$$

On solving this equation for integer m and n we have the prime values p and q. The difficulty in this elementary factoring approach is finding the integer primes n and m when N gets large as encountered in present day cybersecurity. Without loss of generality, we can say that-

$$p<\text{sqrt}(N) \qquad \text{and} \qquad q>\text{sqrt}(N)$$

This is equivalent to saying-

$$n<[\text{sqrt}(N)-1]/6<m$$

From it we deduce that p is less than 177 for the N being considered. Next applying the search program-

for n from 100 to 177 do ({n,(187162+n)/(6n-1)})od;

This produces the integers n=133 at m=235 in a split second. Thus we have the prime factors-

p=6(133)-1=797 and would q=6(235)-1=1409

Notice that we would have gotten no integer values for n and m if we had chosen p=6n+1 and q=6m+n, although this form for p and q would still have been consistent with N=6k+1. Thus, in general, one needs to consider all possibilities for p and q consistent with N.

What the above result has shown is that very large semi-primes can be factored using the variables n and m which follow from evaluating the algebraic equation-

$$m=F(n)$$

The upper limit on n will be-

$$n<(N\mp1)/6.$$

With the advent of superfast computers including potential quantum computers, the equation m=F(n) will be solvable for integer n and m and thereby make present day public key cybersecurity obsolete.

U.H.Kurzweg
May 27, 2024
Gainesville, Florida
Memorial Day