Breaking RSA semiprimes

Factorial impact on number theory and understanding discreet logarithms

A mouse can eat an elephant but it has to do it a bite at a time.

The security of RSA asymmetric public key systems rests on the belief that no one can solve the problem of discreet logarithms. The factorial process described below is a mechanical process as opposed to a mathematical process. However, they are equivalent because we know this approach can factor a number in a second when we are told that should take a billion-billion years etc.

Our networks are already getting picked apart without having to directly break keys.

The fact that this kind of discreet logarithm problem can be solved with this following mechanical approach that will factor semiprimes means that accomplished mathematicians have a real-case demonstration and description of how a mechanical solution solves the problem. When one of these mathematicians publishes the equivalent mathematical description then they will have achieved a significant milestone in number theory.

This paper was first written about a decade ago for submission to the formal cryptographic archive ePrint. A previous event through ePrint indicated that this portal that controls the cryptographic science publishing space is like too many others and is a system of agendas and hidden agendas. They allowed an unfounded claim to be published on their archives and they refused to allow a rebuttal (the mathematical proof) to be published as a fair response. The ePrint process was easily shaped to self-interest and hidden agendas likely at the level of large corporations and governments. Just as has happened with the Common Criteria and so many certification systems what was intended to be an open forum for scientific discussion has morphed into a gatekeeper.

Because of this, this paper was not submitted for ePrint. It is fairly easy to recognize manipulation when you see it. An additional consideration in not publishing it at that time was it held a different level of riskiness that it might be misused. It is not the same relative observational perspective at this point in time. It is obvious that it is simply much easier to steal keys then to break them.

Rapid Factorization of Prime Number Composites or RSA semiprimes:

A mouse can eat an elephant but he has to do it a bite at a time. It comes down to how fast it can eat.

An alternative to the Sieve Method

Unlike the encryption algorithms submitted to Advanced Encryption Standards competition, Whitenoise is not a free algorithm. We encourage aggressive and widespread testing of Whitenoise. However, any unauthorized use or deployment

Breaking RSA semiprimes

Abstract

This paper introduces a new technique for the rapid factorization of prime number composites.

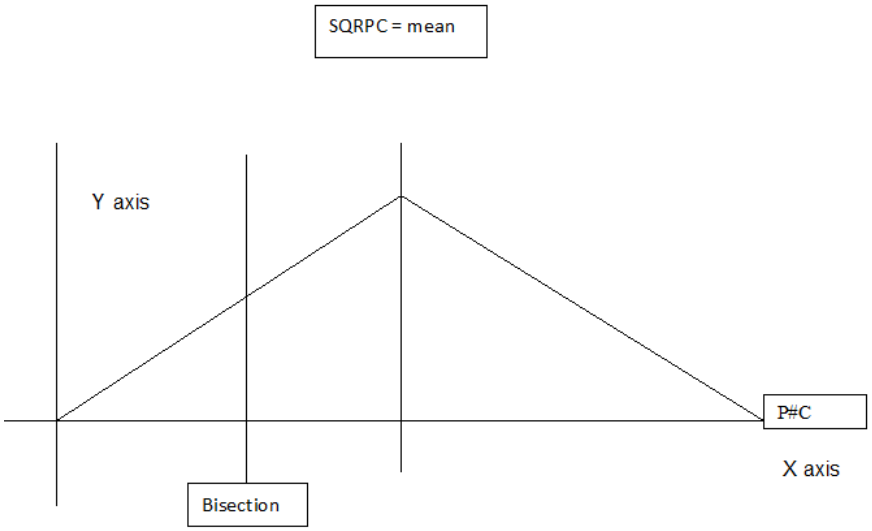
The cornerstone of Public Key Cryptography as well as several other security utilities is the fact that while it is easy for anyone with a calculator to be able to multiply two prime numbers together, it is considered a functional impracticality to rapidly factor the prime number composite into its two distinct factors. Surfing the internet will bring one to many sites where factoring challenges abound and the current prevalent methods for achieving this factorization is either brute force or sieve methods. These techniques are so slow as to not pose any risk for the security of these types of systems.

It was noted that if one takes the 6^{th} derivative of two points within a range on a normal curve, the larger point divided by the smaller point, that the closer you are to the solution the more volatile the remainder becomes. This then becomes the primary criteria in a decision tree in deciding which way to jump if one is deploying a bisection method to try to locate a prime number factor.

On a basic system deploying this technique it is possible to factor a 60 to 80-bit prime number composite in under a second. It is believed that expanding upon this technique will make the factoring of large prime number composites an easy task and hold out great possibilities for the manipulation of primes and composite primes in general number theory. It is to be noted that this is not a simple mathematical shortcut but because of the ready access to computers and even the basic computational speed of a simple desktop computer, it is a technique that should be far superior to existing techniques and hold out great possibilities.

Breaking RSA semiprimes

Rapid Factorization Architecture



If one looks at a Cartesian plane and a [very poor] rendition of a normal curve, the following elements are readily identifiable.

1. We can draw a normal curve with the endpoint of the curve on the X-axis being equal to the prime number composite [P#C].

2. We can take the square root of the prime number composite and this becomes the mean.

3. We know that one of each of the two factors we are looking for will reside somewhere on either side of the mean.

4. Looking at the graph above, we will search for the smaller prime factor of the prime number composite. Our first step is to bisect the smaller area of the curve along the x-axis and in this example it is labeled bisection.

5. First we rapidly test to see whether the point of bisection is a whole number. If it is (unlikely) then we have found one of our factors. If this was the case, we simply divide this number into the semiprime.

6. The challenge now is to decide on which direction of the bisection line we should jump in order to make the next bisection.

It was noted that if one takes the 6th derivative of two points within a range on a normal curve, the larger point divided by the smaller point, that the closer you are to the solution the more volatile the remainder becomes. This then becomes the primary criteria in a decision tree in

deciding which way to jump if one is deploying a bisection method to try to locate a prime number factor.

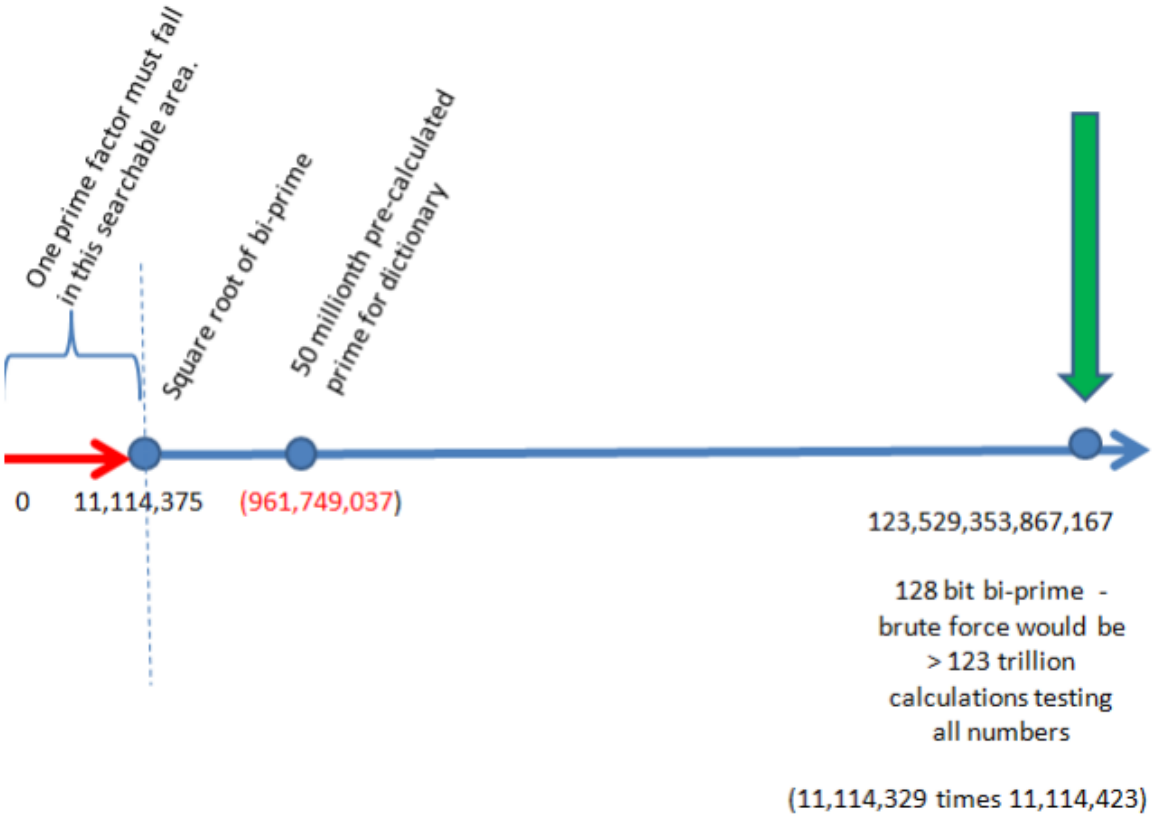
Written by: Stephen Boren email sboren@bsbutil.com

Andre Brisson email abrisson@bsbutil.com

Created: 6/24/2002 Modified:7/24/2003

December 10, 2015

A more recent view from a paper for the Telecom Council of Silicon Valley Deep Dive on Security in the Snowden Era this year 2015 shows this idea on just a number line that is easier for some to see the behavior. It was in preparation for demonstrating this capacity to factor semiprimes that is was sadly recognized that a simple prime number dictionary attack could accomplish the same thing.



It was noted that if one takes the 6th derivative of two points within a range on a normal curve, the larger point divided by the smaller point, that the closer you are to the solution the more volatile the remainder

becomes. This then becomes the primary criteria in a decision tree in deciding which way to jump if one is deploying a bisection method to try to locate a prime number factor.

This nugget, the recognition of starting with a square root of a semiprime and the behaviors of derivatives was a Boren insight.