TCSV Whitenoise Demonstration of Factoring bi-prime public key equivalents

whitenoise
technologies

PRESENTED TO
TELECOMCOUNCIL
SILICON VALLEY

TCSV Deep Dive on Security in the Snowden Era at Microsoft

How secure are we?

The security of RSA style public key asymmetric frameworks is predicated on the premise that the creation of a public key is a one-way-function. This means that it is “easy” to do the math in one direction but impossible to go backwards and unwind it.

It is easy for anyone to multiply two prime numbers together with a calculator but it was considered impossible or infeasible to go backwards and determine the two original prime number values. This process is called factoring.

For a long time RSA ran factoring challenges. Most persons were left with the sense that this validates the security of those PKI frameworks. It had once been very difficult to factor co-primes. It was supposed to take thousands of years to do so.

But there are few if any public key networks using keys of the strength found in their contests. That is an academic distraction.

The majority of networks globally rely on 128-bit keys i.e. SSL, TSL etc. Just trying to move up to the use of 256-bit and 1024-bit keys makes processing problematic and additional resources like accelerators become necessary. The overhead required in public key technology excludes that technology from deployment in the majority of inexpensive Internet of Everything endpoints.

“The **RSA Factoring Challenge** was a challenge put forward by RSA Laboratories on March 18, 1991 to encourage research into computational number theory and the practical difficulty of factoring large integers and cracking RSA keys used in cryptography. They published a list of semiprimes (numbers with exactly two prime factors) known as the RSA numbers, with a cash prize for the successful factorization of some of them. The smallest of them, a 100 decimal digit number called RSA-100 was factored by April 1, 1991, but many of the bigger numbers have still not been factored and are expected to remain unfactored for quite some time, however advances in quantum computers make this prediction uncertain due to Shor's algorithm.”

Shor's algorithm, named after mathematician Peter Shor, is a quantum algorithm (an algorithm that runs on a quantum computer) for integer factorization formulated in 1994. Informally it solves the following problem: given an integer *N*, find its prime factors.” wiki

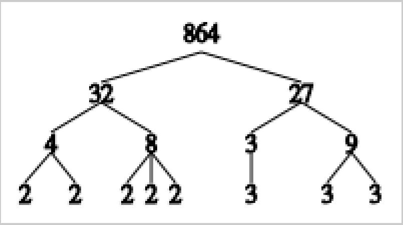
https://en.wikipedia.org/wiki/Prime_factor

https://en.wikipedia.org/wiki/RSA_Factoring_Challenge

Factoring materials

Demo

Just looking at a browser shows that 128-bit public keys are the prevalent available security strength. A 128-bit key is 16 characters long. Since that is what generally is used to protect or communications that is the scale of what we will factor with the Whitenoise Large Number Factorer for this demo.



This image demonstrates how to find the prime factorization of 864. A shorthand way of writing the resulting prime factors is $2^5 \times 3^3$

Note: Whitenoise keys are not susceptible to mathematical or factoring attacks because the keys are created by a mechanical process and they are not dependent on arithmetic functions for security.

See: http://www.wnlabs.com/products/InDenialCodeRedDirect.php

When the public key framework was adopted it was under the belief that factoring public keys was INFEASIBLE and would take tens of thousands of years. Our technique shows that waiting for quantum computing is not necessary to factor public keys. Daily news of major breaches and theft tell us the bad guys already have it figured out.

YouTube video demonstration of factoring co-primes:
https://www.youtube.com/watch?v=GwkwgR_78dQ&feature=youtu.be

Factoring Demo Directions

Fig 1

In the following figure we see the Large Number Factorer utility. Underneath we see a calculator which is found in Accessories in Windows. And in the background we see a page of prime numbers from the following web site:

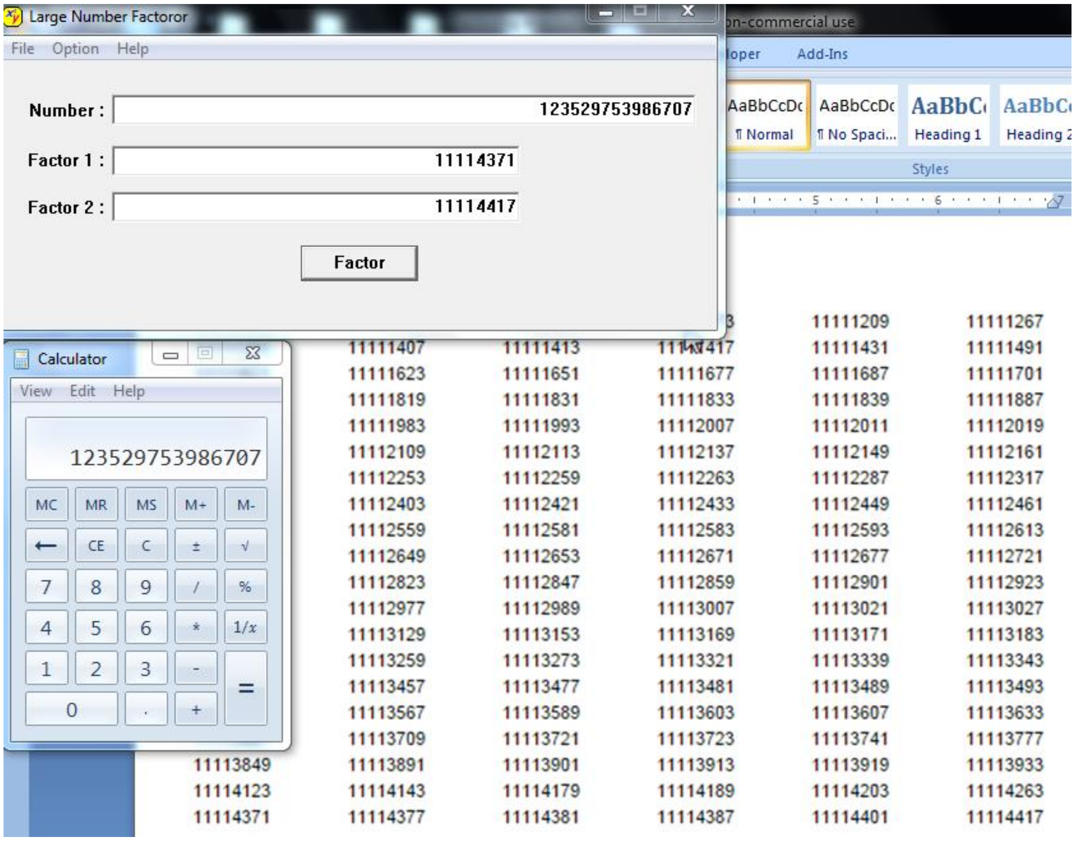
http://compoasso.free.fr/primelistweb/page/prime/liste_online_en.php

We are going to make a co-prime (or bi-prime) product which is equivalent to a public key and upon which the RSA factorization contests were based.

TCSV Whitenoise Demonstration of Factoring bi-prime public key equivalents

The page selected list prime numbers 8 bytes long so that a composite prime (multiplied together) is approximately 16 bytes which would be equal to 128-bit strength keys which are prevalent in global networks. It is not necessary (although possible) to factor 100 byte bi-primes if they are not using them.

In the calculator we are multiplying 11114371 and 11114417 together to get a bi-prime public key equivalent value of 123529753986707. We copy that value and paste it into the Large Number Factorer. When we click Factor it locates these primes in seconds.



Number : 123529753986707

Factor 1 : 11114371

Factor 2 : 11114417

123529753986707

			3	11111209	11111267
	11111407	11111413	11111417	11111431	11111491
	11111623	11111651	11111677	11111687	11111701
	11111819	11111831	11111833	11111839	11111887
	11111983	11111993	11112007	11112011	11112019
	11112109	11112113	11112137	11112149	11112161
	11112253	11112259	11112263	11112287	11112317
	11112403	11112421	11112433	11112449	11112461
	11112559	11112581	11112583	11112593	11112613
	11112649	11112653	11112671	11112677	11112721
	11112823	11112847	11112859	11112901	11112923
	11112977	11112989	11113007	11113021	11113027
	11113129	11113153	11113169	11113171	11113183
	11113259	11113273	11113321	11113339	11113343
	11113457	11113477	11113481	11113489	11113493
	11113567	11113589	11113603	11113607	11113633
	11113709	11113721	11113723	11113741	11113777
11113849	11113891	11113901	11113913	11113919	11113933
11114123	11114143	11114179	11114189	11114203	11114263
11114371	11114377	11114381	11114387	11114401	11114417

abrisson@wnlabs.com