PHUN WITH DIK AND JAYN
BREAKING RSA CODES
FOR FUN AND PROFIT

A supplement to the text
CALCULATE PRIMES

By James M. McCanney, M.S.

RSA-2048 has 617 decimal digits (2,048 bits). It is the largest of the RSA numbers and carried the largest cash prize for its factorization, US$200,000. The largest factored RSA number is 768 bits long (232 decimal digits). According to the RSA Corporation the RSA-2048 may not be factorable for many years to come, unless considerable advances are made in integer factorization or computational power in the near future

Your assignment after reading this book (using the Generator Function of the book Calculate Primes) is to find the two prime factors of RSA-2048 (listed below) and mail it to the RSA Corporation explaining that you used the work of Professor James McCanney.

RSA-2048 =
25195908475657893494027183240048398571429282126204032027777
13783604366202070759555626401852588078440691829064124951508
21892985591491761845028084891200728449926873928072877767359
71418347270261896375014971824691165077613379859095700097330
45974880842840179742910064245869181719511874612151517265463
22822168699875491824224336372590851418654620435767984233871
84774447920739934236584823824281198163815010674810451660377
30605620161967625613384414360383390441495263443219011465754
44541784240209246165157233507787077498171257724679629263863
56373289912154831438167899885040445364023527381951378636564
39121201039712282212072035 7

jmccanneyscience.com press - ISBN 978-0-9828520-3-3

$13.95US NOT FOR RESALE

Α Β Χ Δ Ε Φ Γ Η Ι ϑ Κ Λ Μ Ν Ο Π Θ Ρ Σ Τ Υ Ω Ξ Ψ Ζ

TABLE OF CONTENTS

OTHER BOOKS AND INFORMATION BY JAMES M. McCANNEY, M.S. Physics

www.jmccsci.com for eBooks and hardcopy books

Books and eBooks (some available also in Spanish)
Planet X- Comets and Earth Changes
Surviving Planet X Passage
Atlantis to Tesla–The Kolbrin Connection
Principia Meteorologia – The Physics of Sun Earth Weather
Calculate Primes (only available in print version)
The Diamond Principle
Comets
WATER

CDs and DVDs
2 DVD set – Historical video lectures re-mastered to DVD
DVD lectures series – DVDs
CD – 110 high resolution aerial photos of the American Southwest taken from 45,000 foot altitude from Los Angeles to Denver
2CD set – 18 hours - The Physics of Ancient Celestial Disasters
Emergency Survival Re-Calendar Portable Sun-Star Clock

Professor McCanney hosts a weekly radio show heard worldwide on station WWCR – Nashville, Tennessee
"The James McCanney Science Hour – At the Crossroads"

- See www.jmccsci.com for details

I. About the Title and Cover Picture

The first line of the title is PHUN WITH DIK AND JAYN. There is an entire story behind this title. But first go back to first grade reading class if you lived long ago in the USA. There was a book everyone started with called FUN WITH DICK AND JANE. The first line went something like this (and of course illustrated) … See Dick. See Dick Run. See Jane. See Jane run. See Dick and Jane Run.

When I released the name of the current book to the public I did something that I had not done since my first book … that is … pre-release the title before the book actually came out. All of my releases have had pre-sale releases before the titles were announced. I may be the only person that has the ability to sell my books on a large scale before the book title is actually announced due to my presence on many radio shows as a trusted author and guest but also as host of my own weekly radio show The James McCanney Science Hour – At the Crossroads that airs commercial free every Thursday evening from the largest radio station in the world WCCR out of Nashville, Tennessee. But something started to happen with my detractors (those hateful government disinformation agents hired to try to minimize my work). They began sabotaging my releases by creating same of similar titles or as in the case of The Diamond Principle book release, created a widely publicized counter attack book allegedly co-authored by the incapacitated Stephen Hawkings.

So I decided to play a mind game on the highly paid and orchestrated team that is hired by the gov misinformation alphabet soup agencies including the CIA and NSA. I decided to pre-announce the title of this book with the intention of changing it after they made their move. The release of this book was simply the title "Breaking RSA Codes for Fun and Profit". Almost immediately they released a book with the same title, obviously attempting to thwart any notoriety that I might gain on such a controversial topic that they are trying desperately to keep in the box.

Thus I added the first line to the title which no one would possibly duplicate without making it completely obvious that they were copycats in the face of an on looking ever increasingly aware public to the ways of the snooping NSA and their counterpart tech laboratory called RSA which has been heavily involved in government secure computing for decades and for which this book is one small step at demolishing their ability to snoop on the public.

All of my books have a set of attributes. None have the same topic as any of the previous books. They all build on the work of the prior releases but take a 90 degree turn down paths that no one has ever taken before. And lastly and the part that provides some fun for me in my own

devious way … to play with the minds of the world controllers and their teams of mini-minded bought and paid for engineers and scientists who have sold their souls to the devil for a pay check and hopes of maintaining their careers until they can retire and forget about all the damage they have done to their fellow humans.

The title PHUN WITH DIK AND JAYN also has a more hidden meaning. This book is intended to take a turn in the war on snooping. It is an effort to spark a new direction for the public to begin making a direct attack on the attackers. About two weeks before I decided to release this book (supplement to the Calculate Primes book with DVD lecture) there was a secret backdoor contract and meeting between the NSA and RSA Laboratories Company. Protestors marched in front of the meeting facilities and protested the ongoing "information gathering" policies and activities of the NSA. But central to their efforts is a combination of secure computing that allows the government to remain secure while allowing the government to snoop at will on anyone and everyone literally in all communications that you make including cell phone and land line calls, anything you do on your computer and everything you see on the internet. They search and scour all of your emails and have catalogued all your friends on twitter, facebook and all the other "social mediums".

They can go back to conversations you had years ago and can then get other agencies like the IRS to target you for harassment. If they do not like you enough they can simply haul you off the street at any time and fly you to a foreign country detention center for torture, interrogation and "corrective measures" without any due process of law.

Central to all of this is secure computing and this is where the RSA Codes come in. Many decades ago mathematicians developed a method of exchanging secure messages using prime numbers. The assumption was that prime numbers had no calculable patterns and very large numbers would be practically impossible to factor into their prime number components. So well entrenched was this assumption that estimates were made based on existing and potential supercomputing capabilities to determine the level of security that such a prime number based system would provide. (see Chapter XVI. The subsection on "RSA numbers" and the "RSA Challenge" for more details).

Secure government computer systems had to be protected and this was deemed by all the experts as the most secure system. The company RSA Laboratories built a living creating the Secure Computing cryptology "Keys" which were well selected large numbers with only two prime numbers as factors. All was well with this method and the keys were provided by the RSA Corporation to all layers of private and government secure computing for both hardware and software.

As you can see form my bio, I worked in the area of secure computing as a Principle Engineer, overseeing both hardware and software design in some of the most complex computing systems known to man. I was employed for over 10 years in a company that built what are known as "front end processors" FEPs and installed networks for the largest corporations and government installations in the world. They were IBM compatible … for installation on IBM mainframe computing systems and offloaded the network transmission task from the mainframes that then were left to concentrate on processing data for oil companies, banks, and secure government installations.

I was totally immersed in all aspects of secure computing specializing in transmission encryption and computer protocols. This was back in the days when engineers operated high tech companies based on sound engineering, product verification with rigorous testing BEFORE the products were delivered to the customer and high levels of instant customer service. But all of that changed. MBAs came in who were related to stock holders and attempted to manage things they did not understand. Products were released to maximize sales advantage before they were tested and profit became the motivating factor in all decisions.

Additionally, somewhere along the line the world of secure computing took a turn and began to be used to snoop on the public. The platforms like Micro-soft Windows and many applications became the open door for snooping with the government demanding access to any and all computing equipment. Encryption and firewalls that were truly secure were not allowed and many people paid a dear price for resisting the government demands. Of course the levels of control came from much higher than the federal government which was controlled by the paranoid control crazy European bankers. Much later on the waves of social media were bought and taken over by the CIA (the police force of the international bankers in the USA) as well as the NSA and Homeland Security.

People unwittingly gave over all their personal information and all their friends' information via the social networking sites without knowing they were contributing to a grand scale data base that would watch their every movement and track everyone they communicated with. At the heart of all of this was the ability of the government to snoop on all citizens all the way up to and including foreign diplomats. The government had secure computing resources but you the public were not allowed to have any semblance of secure computing (although companies sold the concept and the public bought it hook line and sinker). The gov hired companies to create secure computing for transmission encryption as well as firewalls to protect government computer systems and networks. At the center of all of this were the RSA prime number based encryption Codes. ALL OF THIS WAS DESTROYED when my Calculate Primes

book was released since the one and only method of encryption that was used was the RSA prime number method. It was everywhere in hardware and software. This will be explained in more detail later in this book.

Frail home computer anti-virus protection programs also provided easy access for government agencies to look into everything you were doing on your computer as well as monitor all your emails and social networking communications not to mention building a personal profile that could be accessed by anyone in high level government positions. The public became nothing more than lab rats in a maze of sloppy computing "security" and social networking applications. Rather than shut down the internet the government gained control of it to control the public through 24 x 7 monitoring and surveillance as well as social engineering and mind control . This was done in the name of protecting against "terrorism" but the real reason was to monitor and then shape the public to prevent an uprising to fight the onslaught of tyrannical government gone amuck as the new world order was moved into controlling every aspect of your lives.

II. Preface to Breaking RSA Codes for Fun and Profit
Preface by the Author

Breaking RSA codes that have been the key to modern secure computing encryption for both transmission and for internal software and hardware protection against hackers and other unwanted intruders is an offshoot of my resolving the oldest unsolved mathematics problem … that is … to not only put order to the prime numbers … but to understand their patterns so that very large prime numbers could be calculated easily.

Part of this solution involves the fact that with the new method the primes were calculated not one at a time but in large groups. Additionally you did not have to calculate ALL the primes but could target a region of the number line and calculate the needed prime numbers in that "zone". This led to the simple and quick factorization of large numbers. Other aspects to the RSA codes' use of the sizing of prime numbers and factors also played readily in the new technique. Those aspects made it difficult to crack the codes using advanced supercomputing techniques BUT oddly enough made it extremely easy to break the codes using the methods I had developed to directly calculate prime numbers.

The RSA codes depended on a number of assumptions. An extremely large number with just two prime factors was calculated using modern super computers. Just locating two large primes was considered difficult in itself but to reverse the process was even more difficult. That is, to take the large number and factor it into its two prime base numbers was considered to be a monumental task because all of this was done with brute force calculations. All this will be explained in detail in this text.

The assumption based on the long history of mathematics was that the prime numbers were at best random and had no order and therefore had to be laboriously calculated using vastly expensive super computers. No one in their wildest dreams ever imagined that someone would crack the oldest problem in all of mathematics to directly and easily calculate prime numbers. So inherent in the encryption industry was this assumption that a very boastful attitude surfaced stating the number of thousands of years of super computing power that would be needed to break the codes. The codes were used in all levels of secure computing from internet transactions to the highest levels of government agencies and military security including military satellites both hardware and software.

With that in mind, understand that the solution to the problem of understanding the prime numbers was at the core of the ability to break the RSA codes. This is a complex field but after reading this short pamphlet you will understand the history and current affairs regarding encryption

and how it affects you as the man on the street trying to survive in a world that gets more insane every day.

My public release of the book Calculate Primes occurred in March of 2007 (see Chapter XVI for more details on the book release) and immediately rocked the world of secure computing. It was immediately recognized that the extensive use of RSA codes in all levels of secure computing was in big trouble. Extensive efforts were launched on all fronts culminating in an announcement by the head of Homeland Security that all of secure computing was in chaos and they had no idea how serious the problem was, nor did they know how to fix the holes that existed in all levels of computer encrypted transmissions and firewalls. Just weeks after the book release the RSA Laboratories revoked all of its previously announced prizes for resolving large encryption key factors (see Chapter XVI for details). The Electronic Frontier Foundation which offered the Cooperative Computing Awards for finding the largest prime number created a new rule banning the use of the McCanney Generator Function from being used to generate large prime numbers and claim their prize money. Now the prize claimant had to be pre-registered with them and had to prove that they used the "official" specified computer algorithms.

There was a huge amount of denial in the computer industry although those who were at the heart of the issue in the military and other secure agencies realized the depth of the problem. Vast teams of computer specialists worked day and night in attempts to plug the holes in secure computing. The only problem was that in the development of secure computing the programmers or hardware designers are always compartmentalized and their work is kept in small groups so literally no one had any idea where all the locations of RSA codes were located let alone how they were programmed or implemented, making it literally impossible to fix the problem … thus the Michael Chertoff announcement as head of Homeland Security that all of secure computing was in chaos and they had no idea how to assess the problem let alone fix it. I personally was contacted by dozens of computer specialists as well as attorneys representing corporations including the RSA Laboratory seeking more information on the new released information. Engineers and computer specialists from many companies working on secure computing encryption codes contacted me directly for detailed discussions.

As a caveat many may wonder why I would release a mathematical problem that caused such destruction of the secure computing industry. The answer is simple. I was doing the public especially a huge favor. If this information had fallen into the wrong hands and I had not made it public in standard security agency fashion they would have buried the information and pretended it did not exist. The real damage would have

occurred when hackers eventually would have invaded all of secure computing and no one would have known about it until all of the damage was done not only in private industry but also all the way to the highest levels of government and military computer and network security.

There was oddly enough a complication that occurred in the world of mathematical analysis and high level mathematics. Just as the Calculate Primes book was being released to the public the Field Foundation was awarding its latest prize in mathematics to Terry Tao and Ben Green for writing a paper that allegedly had proven that there were no long term patterns for the prime numbers and that therefore the prime numbers were random. My book Calculate Primes destroyed the Tao-Green work but the problem was that in the world of peer review mathematical journals, there was a high level conflict of interest as Tao and Green were considered the "experts" dealing with patterns in prime numbers so they blocked the publication of the Calculate Primes work which proved conclusively not only that the prime numbers have distinct patterns but presented an equation The Generator Function to directly calculate all of the prime numbers to infinity, relating them to earlier "families" of primes.

The prime numbers indeed had complex patterns that were readily understandable by anyone with a rudimentary knowledge of arithmetic. They additionally had many standard mathematical properties including symmetry, reciprocity, closure, and many properties of closed groups. There is no question that the Field Prize should be retracted but in the politics of ivory tower peer reviewed snobbery I doubt this will happen any time soon. This partly also is because the history of dealing with prime numbers has wallowed in the area of what is called "Mathematical Analysis" which I have publically stated will never bring concrete results regarding prime numbers. In fact in dealing with more esoteric problems such as the unsolved Twin Prime Conjecture Tao himself has stated that the limitations of Mathematical Analysis will not bring final solutions, but that is another matter not directly related to the present book.

The following discussion of my history of working on prime numbers is derived from the Calculate Primes book to which the current pamphlet is a supplement. Note that you do not have to read that book to follow the basics of Breaking RSA Codes but if you are serious about attacking the problem as a mathematician or computer hacker you will have to read and understand that book. To learn how to break RSA codes for fun and profit you first have to understand the history of the solution to the problem of easily calculating prime numbers.

The solution to the prime number problem haunted me from my earliest introduction to it in late grade school or early high school. I had worked on trying to find patterns and certainly found myself "discovering" many of the same facets of the prime numbers and following many of the

same false leads that the hundreds of mathematicians had stumbled upon over the past 2500 years.

In pursuit of a solution over many decades, I read everything that existed and got to know the paths of great mathematicians such as Gauss, Euler and Riemann, the same great names that brought us so many unbelievably complex advancements in every field of mathematics. Certainly the solution to understanding the primes had its base in the foundations put down by these greatest of mathematicians. My efforts of course came and went as I worked on other pursuits. I had to leave my prime number file on the shelf to collect dust only to return time and time again to take up the battle.

Then finally a number of years ago I sat and stared into a mental mirror and had to come to task with a fundamental issue. If all of these great mathematicians could not solve this problem, were they all wandering perhaps down the wrong roads? What were they all missing? I decided at that point on two issues, both of which later proved to be correct. The first was something I had discovered while wandering in the rain forests of Central America and camping in the remotest wilderness areas of northern Canada. This was the realization that the solution to understanding the prime numbers was like everything else in nature … it most certainly did exist … and it had to be elegant but simple. And secondly, there had to be a new "method" of mathematics that had not yet been discovered.

As I later found out, I was correct on both counts. So it was at that fateful point in my theoretical life that I made a conceptual decision that was the equivalent of cutting off my right arm. I would take indefinite leave of working on the project labeled "Prime Number Problem" … until such time as I had forgotten all of what had to be false leads of all these other mathematicians I had studied and likewise abandoned my own set of false leads.

Many times I had to resist the temptation to reopen the "Prime Number Problem" file as I saw it sitting on the shelf, since I had not shed myself of all the dead weight yet. Patience my son, patience a little voice said inside of my head. And I then continued with the many other pursuits that have kept me more than busy over the years.

Then one day, after possibly 2 years of not thinking about the prime number problem, I sat down with pen and paper and the solution starting flowing like water over a newly opened reservoir. I was setting on a deck in the warm sun, and with a fresh supply of paper, began putting together the pieces of the puzzle. In retrospect, at times I thought that there was one or another aspect of the total solution that was paramount or more important than any other, but in the final analysis there are so many subtle and intricate solutions that have to be woven together to make the final

solution work, that it is not possible to weight any one aspect above the others. As with many events, it was a collection of factors all working in harmony to give the true vision of the prime numbers.

Little did I know that my brains had been purged of "the past prime number problem" information and the fresh look was truly what was needed. As I sat down that morning with pen in hand, I began probing into the middle of the prime number table. It hit me like a ton of bricks and I did not stop working until the entire solution method had been worked out … it was so logical and so simple … and so elegant … I had solved the initial portion … the essence of the prime number problem. It took another 6 weeks of daily work to iron out the details and put it into a form that other people would understand. Additionally I had to answer for myself all of the difficult questions I knew that professional mathematicians would ask when they saw the formula that directly calculates the prime numbers. Most of all, I had discovered a new mathematical technique that I knew had to exist and may possibly be used on other more complex mathematical problems.

This book has been designed for the general public and also for mathematicians who want an overview of the solution to the oldest and most elusive mathematical problem in the history of modern man. The supplemental text "Breaking RSA Codes for Fun and Profit is one of the practical applications of the original work on prime numbers main text Calculate Primes.

jim mccanney

P.S. on an internet blog one of the nameless government shill trolls that hang out to bad mouth and attempt to divert any positive mention of me and my work had criticized me for spelling my name in all small letters. This is on purpose as I feel a person's fame and notoriety should not be based on a lengthy string of "Dr" " PhD" or corporate/government alphabet soup agency affiliations or other letters that are meant to impress like metals on a General's chest … to the contrary one's stature must be measured by what you say and your ability to communicate it to your audience … I have my well earned degrees and extensive work background of which I am very proud … all this is well and good … but I write my name in small letters so that each of you can be the judge

.

III. About the Author

This book, as promised, will present to the public a rarely seen side of the author. James McCanney is known worldwide for his research and books as well as radio and lecture appearances dealing with the electrical nature of the cosmos. What many people do not know is that he is also a Mathematician who has worked on and solved some of the more complex problems of Physics and Mathematics, and is an expert in computer design, solid-state physics, telecommunications and computer protocols.

He has worked about half of his lengthy career in private industry, owning several of his own companies and also taught at the University level in Physics, Mathematics, Computer Science and Astronomy. Much of this was accomplished in multi-lingual settings, having worked in the USA, Latin America and with high-level Russian scientists. He has presented his findings at numerous international conferences and is a regular presenter at American Geophysical Union meetings. He has presented his theoretical research in locations such as Los Alamos National Laboratories, International Air shows and International Electric Propulsion conferences. Understanding his background is important in placing the current text into perspective.

James M. McCanney, M.S. received sound classical physics training at St. Mary's University (Winona, Minnesota) receiving a Bachelor of Arts degree with a double major in Physics and Mathematics in 1970. He was offered full scholarship awards to three major US physics graduate schools to pursue his graduate physics studies. However, he chose instead to postpone graduate studies for a period of three years while he traveled and taught Physics and Mathematics in Latin America.

During this time he spent a good deal of time traveling to ruins of ancient cities and archeological sites, studying firsthand many times as the ruins were dug from under dirt that had not been moved for thousands of years. Also during this time he developed the basis for his theoretical work that would, at a later date, deal with the celestial mechanics of N-bodies and plasma physics, as well as the groundwork for the current treatise on prime numbers.

He has stated that in his travels he learned that nature provides elegant yet simple solutions to even the most complex problems, and that she reveals these fundamental secrets to only those who pursue truth for truth's sake, without the encumbrances of modern life or economic rewards that so many times cloud the visions of humans, especially scientists, most of whom are entrenched in the age of big business and government monopolized science.

With this new understanding of archeology, astronomy of the ancients,

physics and the world around him, Mr. McCanney returned to graduate school in 1973 and earned a Master of Science degree in nuclear and solid-state physics from Tulane University, New Orleans, LA. His research involved a National Institute of Health research grant (in conjunction with Gulf South Research Institute) to study visible light and x-ray sensitive photo polymers to be used in medical Xerox x-ray machines. The results of his research resulted in patented discoveries. He was again offered a full fellowship to continue on with Ph.D. studies, but once again he declined and returned to Latin America to study archeology and teach Physics, Mathematics and Computer Science in Spanish. He continued his personal work to explore the mysteries of celestial mechanics and its relationship to the planets, moons and other celestial bodies.

At this time a fellow Ph.D. at Tulane wrote in a letter to a professor at another University, "the first observation that comes to mind concerning Jim McCanney is his unusually broad range of scientific and intellectual interests. His mind is a veritable fund of information and ideas on topics as varied as Egyptian pyramids and the classification of mushrooms. His character and morals are of the highest caliber. He possesses an excellent aptitude for design and construction of research and measurement systems as well as a creative bent in understanding and explaining observed physical processes. He is able to engage in significant research with little or no direct supervision. His research experience is such that he could involve undergraduates with minimal outlay of funds. He has the ability to command respect of those in his classes and is able to generate an unusually good rapport with students."

After four years living and teaching at the university level in Latin America, in 1979 Mr. McCanney joined the faculty of Cornell University, Ithaca N.Y. as an introductory instructor in physics. It was during this time that he had access to NASA data returning daily from the Voyager I and II spacecraft as they traveled by the planets Jupiter, Saturn and beyond (as well as data from many other space craft). It was here he recognized that the mathematical models in his theoretical work regarding the electro-dynamic nature of the solar system and universe had its signatures in the new data that was streaming in from the edges of the solar system.

His papers were published at first in the peer reviewed astrophysical journals, but soon he began to receive resistance from the standard astronomical community. Mr. McCanney was removed from his teaching position because the standard scientific community did not accept his beliefs regarding the electro-dynamic nature of the solar system, beliefs that are just now becoming the basis for modern Space Science and Astrophysics.

His innovative theories on plasma physics and a new model for fusion

in the solar atmosphere provided the basis for the electric fields and plasma discharge phenomena that have become the core elements of his theoretical models of the true nature of the solar system in which we live, and which are the fast becoming the basis for every international conference on space weather and space physics.

Upon being removed from the physics department for his then radical beliefs, Mr. McCanney was rehired shortly thereafter by the mathematics department also at Cornell University, where he taught for another year and a half and continued to publish his papers in peer reviewed astrophysical journals. Again astronomers coerced his removal from the Mathematics Department and ultimately he was blackballed from publishing in the astrophysics journals in1981.

His first peer-reviewed paper in 1980 "Continuing Galactic Evolution" (written while he was in the Physics Department but published while in the Mathematics Department of Cornell University) advanced a new technique for solving simultaneous differential equations for the orbits of stars in a galaxy. It is said that only a small handful of people in the world understood the significance of this short but important paper. With a second paper "Saturn's Sweeper Moons Predicted", he was, according the department chairman at the time, the only Cornell Mathematics Department faculty member ever to be published in the peer reviewed astrophysics journals.

During this time Mr. McCanney established himself as the originator of the theoretical work regarding the electrical nature of the cosmos for which he coined the term "THE ELECTRIC UNIVERSE", which today is being proven correct on an ongoing basis by space-probes returning data from outer space. Many of his predictions such as x-rays to the sunward side of comet nuclei, that comet nuclei would be found to have no ice or water frozen on their surfaces and that comets interact electrically with the Sun as well as solar electrical activity affecting Earth weather, have now been confirmed by direct measurements in 1986, 1996, 2001 and 2002 to the present day. Many other more abstract concepts have also been verified.

After the Cornell years Mr. McCanney worked in the telecommunications industry as a Principle Systems Engineer at a major telecommunications corporation designing computer telecommunications equipment, and also ran a number of his own companies dealing with satellite communications and electrical propulsion systems. He attended and spoke at numerous international conferences on the future of space flight using his designs of electro-magnetic propulsion.

It was during these same years that he continued to interact with the scientists at Los Alamos Labs and Goddard Space Flight Center during the era of the first comet fly bys of comets Giacobini-Zinner and Comet

Halley. Throughout the years and the decades, he has always remained an Independent Scientist, never using government funding or positions to further his personal research.

In the mid-1990s Mr. McCanney's work was recognized by a group of high-level Russian scientists at the University at Novosibirsk who had measured but did not understand electro-dynamic effects around Earth and in the solar system. Upon discovering Mr. McCanney's work, they translated all of his papers to date into Russian. These are still being taught at the university level as the leading edge of research in this field. It is only due to the ongoing and intentional efforts of NASA that his work has received such little attention in the western scientific community and press.

In the background Mr. McCanney continued working on the illusive mathematical problems facing celestial mechanics, that is, the unknown method of solving simultaneous differential equations. He believed that nature had provided a simple but elegant method to solve these complex problems that did not exist in current mathematical capabilities. He envisioned a mathematical technique that would be applied and reapplied to generate a final solution. In this respect, many unsolved problems of mathematics and quantum mechanics and even genetic molecular structures would have their solutions in this new mathematical technique.

His search lead to a technique that is the basis for the discovery of the solution to the prime number problem presented in this book, and which now holds promise at solving some of the great mysteries of Quantum Physics as well as Genetics. It is based on the "Mathematical Operators" that the Professor calls "Generator Functions".

These mathematical expressions operate on fundamental units or building blocks of nature such as the numbers 0 and 1 (as in the case of the prime number solution in this book) or atomic nuclei (in the case of quantum mechanics) or atoms and small molecules (in the construction of large organic molecules or genetic structures). According to Mr. McCanney, "the Generator Function is an operator that reflects conditions in nature, it builds up a first layer when applied to the basic building blocks, and then is applied to this construct to form a second more complex structure. The same Generator Function is then reapplied to this result and the process continues, with each successive application modifying the prior set of results".

This leads to questions that are being asked for the first time. For example in genetics, could the makeup of the human biped be not only duplicated somewhere else in the universe, but is the norm rather than the exception based on "Generator Functions" that operate on the building blocks of life. Could this pattern be replicated on the far side of the universe just as a diamond would appear the same in such a distant place?

On a simpler note, as the prime numbers would be discovered by intelligent beings on the far side of the universe, they would follow the same mathematical Generator Function that we would discover here on earth. The implications of this new mathematical technique may someday very well overshadow this initial application and the discovery of the formula for directly calculating the prime numbers to infinity as presented in this book and DVD lecture (Appendix I contains the original mathematical treatise).

An essential aspect of the Generator Function concept is that it creates intermediate or "false" solutions that are necessary steps to generate the final correct solution. This is possibly but one of the reasons why so many mathematicians have worked around the prime number problem without finding a solution, as they failed to see the total picture as presented in this book. Countless mathematicians have come to the conclusion that that prime numbers are random with but passing patterns. This book proves that to be incorrect. When you finally look at the prime number table and see why every number is there and how it is related to all the other primes, with all of their "ancestors" bridging back to the numbers 0 and 1, you will understand the powerful impact this book will have on the future.

This is a brief but incomplete history of the background that makes "The Professor", as many people call Mr. McCanney, a person with a unique background and qualifications.

Mr. McCanney airs a weekly radio show "The James McCanney Science Hour – At the Crossroads" heard world wide on short wave radio and also broadcast on the internet. He has been a popular regular guest on many national and international radio shows. Most people know of "The Professor" from his work regarding the electrical nature of outer space and its relation to our planet and human beings that inhabit our blue planet.

He has worked over his career on the current topic of the prime number solution and has taught the following mathematics courses at the University level (in addition to Physics, Computer Science and Astronomy); Abstract Algebra, Linear Algebra, Matrix Algebra, Probability and Statistics, Statistics for Computing, Mathematical Logic, Theory of Numbers, Calculus I, II and III, Engineering Math I and II, Advanced Topics in Geometry and Topology.

He has been an avid student of the history of both Physics and Mathematics and has studied the past to understand what is of greatest importance in the future of these fields of study. The present book is a glimpse into this rarely seen side of Professor McCanney. He has stated that his greatest discoveries to date include the cause of surface fusion on the sun, which gives rise to the solar electric field that drives the electrical nature of the solar system. His second great discovery, which was published almost 2 decades before its discovery, was the prediction that

comets would produce x-rays far to the sunward side, as well as the electrical nature of comets and the prediction that comet nuclei would not contain water or ice, but would be hot dry asteroid type bodies (a prediction that has repeatedly been proven by subsequent space probes), much to the surprise of professional astronomers.

A third major theoretical discovery, which has been observed both in nature and subsequently measured in the laboratory, he calls "The Induced Electric Dipole Red Shift". This is an effect on photons of light moving through a non-uniform electric field that causes both a red shift as well as a bending of light. It also explains the previously unknown cause of pair production (electron-positron production) in photons passing near heavy atomic nuclei. His theoretical work then restructures the laws of cosmology based on this new form of red shift.

And last but not least, his work has rediscovered the work of Tesla and further provides a theoretical basis for deriving unlimited electrical energy from the ionosphere. Another result of his decades of research has been the realization that severe earth weather including hurricanes and tornados are powered by electrical discharges from the ionosphere to the clouds in storm systems. The list of scientific discoveries also includes an electromagnetic propulsion system for use in space travel that has been field-tested.

In spite of these discoveries that were confirmed in many cases decades after Mr. McCanney's theoretical predictions were published, he now has stated that the current treatise on prime numbers potentially may have the greatest significance in the history of both Physics and Mathematics. The solution of the Prime Number Problem has eluded every great mind since the Greeks first defined it nearly 2500 years ago. Cauchy, Gauss, Riemann, Euler, and countless others spent their entire lives scouring this problem, yet could not crack the fundamental problem of being able to directly calculate the prime numbers. Countless major unsolved problems in both Physics and Mathematics base their solutions on the prime numbers, yet no one could directly calculate these illusive and perplexing numbers, that is, until now.

It was in quest of this solution and the understanding of its importance that has brought us to herald this work, which is now explained in a way that only the good Professor can do, making it understandable by anyone with a rudimentary knowledge of mathematics. The solution is simple and elegant, the way nature intended. a.s.

Note to professional mathematicians and scientists: *This text was written for the general public and can be used by professionals to gain insight into the process if directly calculating the Prime Numbers; however, the rigorous 7 part proof can be obtained by emailing the staff at* ***www.calculateprimes.com. Visiting lectures are available.***

IV. How to Use This Text

You will find that this book gives you the fundamental ability to easily find factors of large numbers that qualify as the type of numbers used by the RSA Laboratories for secure cryptography keys. One of the other factors in breaking these codes will be your ability to rapidly jump from one set of numbers to another.

In Chapter XVI the entire set of public "prize" RSA codes are given which will give you some solved examples plus many unsolved examples of large carefully selected numbers that have just two factors that are about the same size. Remember that the RSA Laboratory boasted prizes for the resolution of the factors of these numbers which amounted to a total of over half a million dollars US currency which were retracted and taken out of prize money status just a few short weeks after the release of my original main book Calculate Primes in March 2007. The entire listing of remaining numbers plus their "excuse" for removing the prize money is listed also in Chapter XVI.

Basically you are learning how to use the Generator Function presented in the book Calculate Primes and the quick and easy way to find factors. Note that the traditional method uses brute force computation by large supercomputers to find the factors. With the method given here you create tables of prime numbers in the region in which you are looking for prime factors and search for the prime pairs that multiply to equal the large number "key". It is an entirely different process than factoring.

I have talked about this many times on past radio shows with enough detailed information for anyone familiar with the encryption "key" methodology to readily break the codes. This book is the formal public statement on exactly how to do this. What is missing here is a tutorial on hacking into secure computing systems or all the other devious and malicious things one would have to do (many of them illegal) in order to actually for example snoop on the snoopers. But that would be your choice. What I am actually illustrating in this book is a mathematical model and practical application of an amazing mathematical solution that allows anyone to readily calculate prime numbers out to any given size AND TO UNDERSTAND WHY THESE NUMBERS ARE PRIME and the other numbers are not.

Now if you are not mathematically adept do not worry, this book is also for you because it is important for you to see the numbers in action so to speak and learn about encryption codes and the assumptions that have allowed so many to be fooled into depending on them and the twists and turns of new discoveries that can over night change what was once the

most secure computing encryption system known to man and change it into a whimpering child's toy.

When we look at staggeringly large decimal numbers we are somewhat in awe. I have pointed out many times that the base 10 (or any base modulo number system) is woefully unable to express large numbers. They simply become large numbers with no real meaning just as large words become over burdening to our limited human minds. This is an entirely separate issue but what you will find in this book is how to lose your fear of these large numbers and conquer them with ease. It would be something like flying … once you are over 50 feet above the ground it is all relative. Another example would be swimming over your head … once you are in water over your head it does not matter whether it is 10 feet or a hundred feet … if you can't put your feet down you better start swimming.

Think of this book as a giant joke on some arrogant government agencies that developed secure computing techniques not to protect the government from a foreign spy … but to protect their handlers in the world bank from the public rising up and destroying them and their greedy systems of control that are enslaving the world population today. Also think of it as a first step in David battling the larger than Goliath secure computing monster that we have paid for with tax dollars to protect us from foreign invaders but which has been turned on us the general public.

In the greater scheme of things, there are many more encryption systems available NONE of which are truly secure. I have an expression that if you live by encryption you will die by encryption. If you connect to the internet you are subject to hackers and even automated hacking programs that search for ways to enter your computer. The government is no different.

The issue with Snowden taking vast amounts of secure documentation from the NSA was a blessing to all in the world as it bypassed the need to hack into their databases. His releases exposed the NSA for the lies that covered its snooping of the public. At first they denied it. Then under increasing exposure they tried to state it was only aimed at terrorists. Under further scrutiny it surfaced that they were literally recording everything that EVERYONE did all the time. At this point they tried to justify it claiming they were protecting the public from terrorism. Snowden should be raised to the level of a national hero yet to the government and their crony news agencies they sing a different tune.

There is a literal information war going on and there are not going to be any winners when the smoke clears. For sure the public has already lost and this extends to control of little things like world water and other resource rights. At the core of all of this is secure computing and the survival of freedoms for the individual over oppressive tyrannical out of control governments who are just middle men for the international banks.

V. Coast to Coast AM and Brad Walton Interviews

The official release of the original book Calculate Primes took place on March 05, 2007 after an extensive review of the work by carefully selected engineers and other people with an interest in secure computing and pure mathematics. It was during this review process that I realized that the book by itself would be difficult for the average person to follow so I created the 3 hour DVD lecture that was placed in the front cover of the book.

To date all of my official book releases had occurred on the Coast to Coast AM radio show with host George Noory. I was one of the main regular guests on this show and had been a regular guest also on the original Art Bell show that had grown over the years to become the top rated radio program in the world before it was purchased by Clear Channel and transitioned into the format heard today. All of my releases were planned such that the title was announced on the release radio show and were preceded by weeks of pre-release sales so the public would receive their book the same day as the release occurred on the radio interview.

I used this to my advantage with the release of the Calculate Primes book with DVD lecture. The reason a pre-release was important for this particular work was because I knew that breaking the cryptology key method of encryption would not be a very popular thing to do … especially with the RSA Laboratories and its fleet of high order business and government security contracts.

Not only that but I knew the inner workings of the security agencies and if for one second they imagined that someone had this kind of information they would have most likely come out and kidnapped me, buried my work and thrown me in a hole in the ground. Remember that all I had done was solve a mathematical problem. But it was not just any mathematical problem. It was the most sought after prize in all of mathematics.

The assumption that this problem was beyond the reach of modern mathematical techniques goes back to the ancient Greeks who understood the problem and every mathematician and physicist since most of whom spent vast amounts of time trying to understand the rhythm and patterns of the prime numbers but failed. A secondary problem called “The Riemann Hypothesis” was the most hailed unsolved problem in mathematics holding a $1,000,000 US dollar prize and was the great white hope the solution to which was hoped would shed light on the order of the prime numbers. To this date the Riemann Hypothesis remains unsolved and its importance has been diminished since a completely different solution is

now available to directly calculate prime numbers and which additionally gives a complete understanding of the primes and their order.

So inherent was the difficulty of resolving the order and direct calculation of the prime numbers that there was an assumption by the RSA Laboratories and all of their users and in fact the entire encryption industry both theoretical and practical that they rested compete confidence in the system whose main pillar was that prime numbers had no patterns and could only be discovered with large supercomputers running vast amounts of algorithms to determine the factors by brute force.

Having been a Principle Engineer overseeing all of both hardware and software in the development and production of the most complex computing machines ever made (which offloaded the IBM mainframes from the communications networking security functions), I was in a unique position to understand the consequences of solving the prime number problem. I also had the mathematical background which most engineers do not have who may have been in similar positions in the electronics computer industry. Recall that I had been working on the prime number problem since high school and it was one of my life goals to crack that puzzle. So when I finally did solve the problem many years later and was ready to release the information, I knew exactly what I was dealing with and the reaction that would result in the secure computing community not to mention the military and other industries that depended 110% on the factorization prime number cryptology key codes.

My point is that my ability to release and pre-sell a book prior to the title being released was essential to getting this information into the hands of the public prior to it being available to the encryption security industry not to mention the security branches of the government who had a huge stake in keeping this information from ever surfacing. So when the release date came I had one copy of the book hand delivered to George Noory the Coast to Coast AM host and he was the only person on the planet to see the book before that night's interview. The other thousands of copies purchased by listeners (who had purchased without knowing the title) were on their way and there would be no way to stop the vast distribution of this information.

Before every major interview I would send a detailed email to the talk show host to read before the interview and to be used as notes during the interview. The copy of this email is contained in Chapter XVI of this book along with other information regarding RSA encryption issues. Many people have no idea regarding the level of pre-show work that goes into a major show like this on both the part of the author and the talk show host to give a coherent review of the complex topics.

During that interview a caller who obviously knew what he was asking called in and asked how this affected the RSA codes. I answered that it

basically destroyed the world of secure computing. One can only imagine the damage that could have been done if this information would have fallen into the hands of the secure spook agencies of the US government who would have first buried into top secret status but undoubtedly within a short amount of time would have filtered out into the rest of the world and all the real damage that would have been done. Releasing as I did forced them to instead face the problem head on and fix the broken encryption systems. That is exactly what happened in short order as I received many calls from engineers from all branches of military electronics corporations to understand the issues involved. As for the RSA Laboratories they responded by removing the prize offerings for resolution of their large numbers with two prime factors (see also Chapter XVI for further details).

The second release of this book occurred with an interview by host Brad Walton of WCCO radio Minneapolis who was a fan of mine as well as a talk show host who had interviewed me many times on the vast number of topics that I cover from economics to space science to the more esoteric topics like “Comets as the Christmas Star” or the release of this book Calculate Primes. A recording of this interview is found on my web page at the URL internet link found in Chapter XVI. I also used the same email brief that Brad received prior to our interview as well as his reading the book and private conversations prior to the interview.

This interview occurred after the Coast to Coast AM book release interview. Also as with all of my book releases I had used many of my own radio show hours to prep the public for the release of this book. Along with the release came my public release of a side of my professional history that never surfaced during the decades of public notoriety regarding my worldwide fame for work on the electrical nature of the solar system. This side of my life always remained private as I had spent about 10 years of my career teaching Physics, Mathematics, Astronomy and Computer Science at the University level and another 10 years working as a high level engineer in the esoteric regions of secure computing and telecommunications including encryption and private networks for some of the largest corporations in the world and government military computer installations.

This was a complex information release that required a complete knowledge not only of the subject matter but also of the agencies that would have blocked this with all the resources at their disposal if it had released in any other “normal” manner.

Today the industry remains in complete denial of the fact that these encryption codes have been broken. This book is your guide to understanding the issues and the methods of breaking the codes.

.

VI. Calculate Primes – the Original Text

Is there anything more fundamental to our lives than numbers? Almost everything we do is based on some form of numbers or can be quantified. Without them we would not have commerce or TV or carpets under your feet. We would not have roads or bridges that do not fall down (at least most of them) and we would not have a way to transfer information from one person or business to another.

YET !!! the most rudimentary aspect of numbers has gone unknown since the time when numbers were first introduced into western society with the Greeks. Other societies developed complex number systems such as the Mayans and our own base 10 number system has its roots in the Arab countries. The Romans developed a number system based on symbols but it was crude and unmanageable with respect to addition and other higher forms of manipulation such as multiplication. Concepts such as square roots or higher math were out of the question because of limitations of the number system.

Western man has used the base 10 number system and almost all of modern mathematics uses it as a base. Numbers like π and e (the basis of natural logarithms) are expressed in terms of base 10 numbers. I am sure that most mathematicians are very comfortable using these and literally all of Mathematical Analysis dealing with the prime numbers is based on the assumption that base 10 number system is all that is needed.

In my work discovering the nature of prime numbers I discovered that the base 10 number system was inherently lacking in its ability to express large numbers. For example the number on the cover page of the present book has 617 decimal (base 10) digits. To most it looks like an awesome number and why would this number be recognized as a number having just 2 prime factors. The answer is that there is nothing inherent in the number that would give you half a clue. Thus the assumption of the RSA Laboratories and the extreme amount of mathematical analysis that goes into the theoretical basis of modern cryptology and the encryption "keys" depends on the inability of anyone to reasonably decipher the factors of large numbers.

Not only did I solve the prime number problem by creating The Generator Function but I also gave an understanding to large numbers. They were no longer out there on their own as long strings of digits. They had a place and relatives and families. Prime numbers were not calculated one at a time but in large groups that were the result of the Generator Function operating on prior groups of prime numbers starting with just the numbers 0 and 1. The entire process of factorization was redefined and instead of searching long list of smaller numbers and dividing them into

the main large number to identify factors (or lack of factors), you simply added or subtracted certain other prime numbers from a special group of numbers that I called the "Magic Numbers". Additionally every prime number had ancestors and future generations of prime numbers would be based on each known prime as the process continued to infinity.

There was another twist to the process … one did not have to generate ALL the prime numbers out to a certain desired point but you could just generate the primes in a designated region of the number line. All of this makes it possible to rapidly and efficiently break the seemingly large RSA numbers into their factors. In fact, many of the more advanced topics remain unpublished as the public can only digest this in smaller pieces.

In the original release of the book Calculate Primes I only wrote 4 pages on the topic of encryption codes. It was just a small offshoot of the main treatise dealing with a practical application that had a major effect on an esoteric branch of the computing world but which affected everyone in the modern world in a major way.

This supplement has been waiting for many years to be released but now with the NSA and RSA Laboratories recent secret backdoor contract and the furor that has been caused by the NSA snooping on the public it was certainly time to release this additional information because people now had a frame of reference with which to put this complex topic.

Numbers were no longer just long strings of digits. They had a place and a reason for being there. The prime number table was no longer just a list of numbers that were missing from the common multiplication table. They were no longer, as one mathematician described them, a seemingly random set of lottery numbers. The prime numbers comprise their own closed system of numbers with many properties such as symmetry, reciprocity and closure. Certainly these are properties only associated with the most organized of mathematical systems and I guarantee you NO ONE in the math world ever imagined that the prime numbers would have such properties.

It is good that there is an application of this process (breaking RSA encryption codes) that will be highly visible to the general public to bring this out of the shadows and into the lime light. But there is an unfortunate side to all of this. In the efforts to keep this work from the public it has been essentially blocked from the schools and young math students just starting to understand numbers. Prime numbers are still being taught as the ancient cave ages concepts of yester year. There are however thousands of home schooled kids and some brave school teachers that are using the Calculate Primes book as part of their curriculum and I see and hear about the results all the time. I hear of the joy of the teachers and students as they realize numbers are not just long strings of digits, but have families and relatives that can be understood.

The table of contents is placed in chapter XV. The current text on Breaking RSA Codes can be read without the original text BUT if one is truly interested in working on breaking RSA codes and understanding the nature of prime numbers then the original text is required reading.

It is important to understand that when I study and move in directions I am not just shooting at random in the dark. Throughout my career I have always studied the history of science and mathematics. I grew up in the computer age before there were any computer courses. I literally watched as the progressive steps occurred from single canned transistors and circuit boards (as in the old Cray computers soldered together by Minnesota farm women) to the integrated circuits and miniaturization to the level we see today. In mathematics I studied the equivalent of a complete mathematics major as an undergraduate complimenting my Physics degree and eventually taught literally every math course at the university level in foreign languages.

So when I worked over the years and decades on the solution to the prime number problem it was not by accident. I realized it was the central most important problem in all of mathematics for the past 2500 years. Unfortunately when I solved and released it, it just happened to drop into the middle of huge controversy because of the use of prime numbers in modern encryption methods. So illusive it had been that David Hilbert did not include it in his Centennial problems list in 1900 because no one ever imagined that it would be solved. In its place and at the top of the list was "The Riemann Hypothesis" which he considered the best hope for understanding the prime numbers. The Riemann Hypothesis remains unsolved and as with many analysis problems may or may not hold the key to further understanding the prime numbers.

When I was at Cornell University as a faculty member immersed in the influx of data from space probes that were just arriving from the corners of the solar system I already had my theoretical work well under way dealing with electric and magnetic fields in outer space and what the signatures would look like in space probe data. I also realized that comets could not be "dirty snowballs" and that the fleets of astrophysicists, astronomers and space scientists that populated those hallowed ivory halls had no clue what was going on in the data and furthermore were strapped to the albatross theories from the 1950s trying to put band aids on ideas proposed long before the first satellites left earth's surface to explore the great beyond.

The point is that once again I was in a unique position at the right time in history and was able to push the limits because I had chosen to study the most important physics topics before the data presented itself.

Regarding the original text Calculate Primes the rear page of the original text is copied onto the next page.

THE FOLLOWING IS FROM THE REAR COVER
OF THE MAIN TEXT BY THE SAME AUTHOR
* RECOMMENDED READING *

- CALCULATE PRIMES -

DIRECT PROPAGATION OF THE PRIME NUMBERS

BOOK and DVD SIMPLIFIED FOR THE GENERAL PUBLIC

By James M. McCanney, M.S.

From the earliest stages of man's existence, the understanding of numbers was deemed to be the most fundamental of concepts. The ancient Greeks developed a counting system based on rows and columns. Almost immediately there was a natural confluence of ideas and thought. But almost as quickly, they recognized a seemingly insurmountable quagmire. When raising the numbers in rows and columns and in the natural development of the counting system, there were certain numbers that refused to appear in these neatly designed sets of rows and columns. These strange numbers were called "Prime Numbers".

Throughout history, the Prime Numbers have baffled every mathematician since the time of the ancient Greeks. Literally every great mathematician has labored and failed to determine the fundamental nature of these illusive numbers. The Prime Numbers seem to follow strange patterns, and then there are large gaps without any, only to have them re-appear again without warning.

Modern computers search for new Prime Numbers with powerful algorithms, attempting to determine the next Prime or Prime Pair. But as these laborious automated searches find more Prime Numbers, there is an ever-increasing amount of super-computing power needed to determine the subsequent Prime.

The method of determining Primes has always been based on the simple definition, that is, a Prime Number is a number only divisible by itself and the number 1. So computers search and factor, by brute force, hoping to find the next Prime. The most important unsolved problems of Physics and Mathematics depend on understanding the Prime Numbers, and to date remain unsolved.

Mathematicians in the 19th century gave up looking for any method of directly calculating the Primes, reverting to higher mathematical techniques to determine such issues as the number of Primes between 2 given numbers, or equations for the "Density of Primes". This has generated the greatest unsolved problem in all of Physics and Mathematics known as "The Riemann Hypothesis".

The research of Professor James M. McCanney has finally cracked the 2500-year-old mathematical problem. This book shows how this age old problem has a simple, but extremely subtle solution in a new mathematical technique that the Professor calls "The Generator Function". This book shows that the Prime Numbers are a unique set of numbers. They can be calculated using only the operations of addition and subtraction, starting with just the numbers 0 and 1. The age-old dilemma of the Prime Numbers has finally been solved. This book and DVD lecture have been produced for the general public to understand the Primes. The original mathematical treatise is also included as an appendix.

jmccanneyscience.com press - ISBN 978-0-9722186-6-5 .

VII. Misinformation Propagated on the Internet

One would think that new discoveries would be welcomed but in the case of the solution of the prime number problem it has been met with severe levels of denial. As already noted it is good that there is a practical application that can illustrate the power of the Generator Function.

Many people use the internet for information but it has become in recent years a cleansed slate with a tremendous amount of misinformation. There was a time when the world "leaders" feared the internet because it gave freedom of communication between people not only locally but also in different countries. Previously "diplomats" were the only ones allowed to talk between countries and citizens were not deemed intelligent enough to voice an opinion. You were only allowed to vote for someone who then appointed someone else to "represent you". Most people believed in the good side of humanity and were totally duped into thinking the negotiations were being conducted in their best interest. The reality was that all of this was a giant dog and pony show to keep the people working as a slave class under the thumb of the international bankers who lived like royalty and literally owned the world. Wars, taxation and interest on phony money was the key to their success, pulling the strings on the puppet governments that dotted the globe (including the good ole USA).

I remember as a kid my adult mentors cursing the "reds" (Russians … a slang word referring to the Bolsheviks who "won" the Russian revolution). The only problem as we later learned was that none of these mentors had ever seen a Russian let alone spoken to one. Only the high level diplomats were allowed to talk and so the "cold war" kept everyone on the edge of their seats for 50 years in fear of immediate and complete nuclear obliteration

The internet changed all of that. It was a powerful tool for many years and it even developed methods for people to communicate daily to all points and people of the world. We woke up to the fact that the Russian guy on the street was the same as us and no more wanted mutual annihilation that we did. To some it came as a major surprise. It also developed things like a free open encyclopedia that allowed anyone to write his input into a subject. Politicians who represent the world bankers (disguised as normal politicians operating in Washington DC) began to call for controls on the internet. But some more devious groups had a better idea. Since everyone was already addicted to the internet and had come to believe everything they encountered there it was easier to take it over and infiltrate it. The open encyclopedia became "cleansed' and pasteurized and homogenized for human consumption. "Standard"

knowledge replaced the open aspect of Wikipedia and gate keepers now monitor for political and scientific "correctness".

Besides taking over applications like google – facebook – Wikipedia – twitter – skype – and a very long list of other popular public open applications they began to use them to infiltrate the lives of everyone that made a cell phone call or connected to a computer. Even if you were not connected to the internet the computer could be infiltrated to store the usage data and report it once you did reconnect to the internet. People were catalogued and the "Big Brother" systems could identify a person even if they logged in from another computer. In facebook "face identification" software (that is also used in public camera systems around the world) would identify everyone and catalogue their friends, with whom and where you had been when you took your pictures. Cell phones with GPS location now needed a google account to work which literally captured and uploaded to a google data base everything that occurred on the phone including tracking the user's location. This was sold as a "benefit" to the user so you could recover all of your phone activity if you ever lost your phone. People bought it hook line and sinker.

Everything that is done today is done with secure transmissions that are encoded and much of it still in use for the common man on the street uses the RSA encryption codes. One might imagine this would be subject to hacking BUT the reality is that for the brief moments that you personally are communicating the codes are relatively secure. The problem is that many large corporations still use the less than secure computing software and encryption methods and you do hear occasionally of hackers breaking into major facilities successfully. Anyone in the secure computing industry should know better but as I said before … he who lives by encryption will die by encryption (a derivative of the old expression "he who lives by the sword will die by the sword").

So if you look for information on the internet regarding prime numbers you will find a host of misinformation and cover-ups meant to dilute the public awareness of the real situation. You get the outdated ineffective RSA code protection that allows anyone in government or fleets of hackers to get into your personal phone and computer whereas the gov and the controllers have better more sophisticated systems.

Chapter XVI has mouse copied information from the internet sources to keep them for posterity and for you to see the level of subtle misinformation regarding RSA codes. For example they officially state that they removed their prize money from the so called "RSA Challenge" within days after my Calculate Primes book release stating that "advances in computing" was the cause. A lot is at stake … money – prestige – egg on some faces – cover up that secure computing is in trouble – etc. etc..

For those who are new to this topic and the more general topic of misinformation in the sciences, after reading this book you have to take a lot more time to review the home page www.jmccanneyscience.com in which all the past radio shows for over 10 years are archived. There is a general "political correctness" in science today. What has happened is that PhDs are granted based on past "knowledge". New concepts become blocked as aging professors rely on past concepts with the PhD candidates learning that the route to success is to repeat what their older peers are telling them. Radical change that upsets the apple cart is strictly prohibited as the new breed of "professionals" work their way up the academic ladder.

Their first published papers are with their name after a long string of other names and after years of steadfastness they are allowed grant research and to have their own topics to pursue. Mentors are at every step of the way guarding the Holy Grail topics that they were taught in graduate school. I have come to call these people "text book geniuses" or "text book repeaters". Many times this is fundamental science but in the case of space science and astronomy, where the theories extend sometimes back to the 1950s, before any modern spacecraft were sent to visit the planets and before modern large telescopes were available, many of the concepts are held more as a religion than science.

Additionally you have to understand that the people you see in the public eye, whether university professors with their lists of peer reviewed published papers and federal grants or scientists who you see in the paper from NASA or other alphabet soup government agencies or related corporations, these are all what I call "Tier II" science. This is what I call the garbage science pawned off on the public which you read about in the news paper, in geee whiz publications such as DISCOVER magazine or on the cleansed internet. The real science occurs in what I call "Tier I". You never see the people or the results of their research. This is the science that goes up the ladder to the world controllers.

As noted in other places in this book, in the field of prime numbers the historical perspective has been in what is known as Mathematical Analysis. Lengthy complex equations that give broad generalizations have taken the place of attempts to directly understand the nature of prime numbers. When I solved the prime number problem I side stepped all of the past techniques and went directly at understanding the prime numbers. One professional mathematician who reviewed my work quipped, "Well, he did it, but he did not use the standard techniques". The person presenting my book to this professor replied, "Yes, that's the entire point".

Relative to the internet one has to understand that there is an ever vigilant oversight of the internet that did not exist even a few years ago. It is extremely important to keep the public ignorant on topics such as the

broken RSA public key encryption codes because the ability of the NSA to spy on you the public depends on it.

In terms of science, my book The Diamond Principle discusses the necessity of the top controllers of the world to keep the public "dumbed down" relative to real science. A great example is the 30 years of watching the NASA Space Shuttle taking off with its great plume of smoke extending into the sky. Everyone is at awe at the complexity of going into space. However, the reality is that the military has had for decades real methods of going into space that do not utilize chemical rockets. The space shuttle is literally a tier II smoke screen to keep the public from seeing the real space program that is doing who knows what in outer space.

Key to keeping the public out of touch with reality is the controlled internet. There is an entire paid group of what we call internet "trolls" that hang out watching for the least mention of taboo topics. These are immediately cleansed or diverted. Broadcast news agencies use the news papers, the evening news along with the internet to give blanket coverage of topics in what I call "social engineering", or shaping public opinion. TV shows and movies round out the misinformation spectrum. I can't count the number of times on TV series I have heard the star (such as Kiefer Sutherland on the TV series "24") state that "256 bit encryption would take more computing time to break than …" etc., etc.. PURE misinformation written into a TV script that everyone was watching and just one more subtle piece of false information to keep the public unaware of reality.

.

VIII. The RSA and NSA … a Union Made in Hell

In February 2014 the annual RSA security conference occurred, which boasts 24,000 attendees and is the premier event of the secure computing year. The RSA Laboratories has turned from the prime number encryption codes for high level secure applications and boasts a record that will make computer center directors confident that they are buying a firewall and transmission encryption protection that literally no one could break into. After all today's corporations have a lot at stake.

HOWEVER before the meeting it was leaked and later confirmed under public denial by RSA that they had signed a $10 million dollar contract with the NSA to provide the NSA a secret backdoor into the secure crypt systems marketed by RSA. With the current furor regarding NSA snooping the backlash effect was immediately felt as over 50% of the attendees and speakers dropped out and refused to attend. Furthermore the event was picketed and protested by groups intent on stopping the NSA from infiltrating anything and everything in sight. It in fact was that meeting that prompted me to release this information on breaking one of the forms of encryption marketed by the RSA corporation and still used by the NSA to hack into the computing systems of smaller users and computer installations (those who cannot afford the higher levels of secure computer protection including you the man on the street). So I am trying to do my small part to continue to hack away so to speak at the gargantuan wall that is the snooping NSA.

The union between the RSA company and the NSA is the last straw of corporate degeneration into the depths of hell. When the company that is marketing their goods to prevent theft of sensitive corporate information secretly sells a backdoor into their product for money and then does not tell their customers … well you take it from there (the same backdoor that hackers could discover and use). Clearly the RSA Laboratories were hiding the fact that their prime number cryptology key system was vulnerable to hackers but continued to hide the reality while making money marketing the system talks for their ethical standards. It finally took the Department of Homeland Security Michael Chertoff to take the podium to make a special announcement that all of secure computing was in disarray and that they did not know the extent of the problem nor did they know how to fix it (referring to the extensive prior use of the RSA prime number encryption products in business and government).

An article appeared in January 2014 regarding the NSA – RSA meeting and is posted on the next page with reference to the source.

Growing number of security experts boycott RSA conference for NSA ties

Published time: January 08, 2014 04:04

http://rt.com/usa/researchers-boycott-rsa-conference-nsa-299/

Eight prominent security tech researchers have announced they will not attend an upcoming industry conference because it is sponsored by the RSA, the company that was revealed last month to have a $10 million contract with the US National Security Agency.

The RSA Conference has traditionally been a major security event, with 24,000 people attending in 2013. Speaking slots at the conference, which is scheduled at the end of February in San Francisco, are especially prized, with program committee chairman Hugh Thompson telling the Washington Post they are "*highly competitive*," often with 2,000 submissions vying for 300 to 400 positions.

This year, however, Edward Snowden's disclosures about invasive NSA surveillance programs have already cast a shadow over this year's event. Reuters reported in December that RSA, one of the most influential encryption companies among customers seeking to hide their internet activity, accepted $10 million from the NSA to make an agency-authored algorithm the primary technique used to generate random numbers in an RSA encryption product.

This algorithm, dubbed the Dual Elliptic Curve, effectively gave the NSA a "*backdoor*" it could use to monitor users who thought they were using RSA's product to hide from prying eyes. When Reuters published this information, RSA claimed it had never asserted it had no relationship with the intelligence community and refuted accusations that RSA intentionally weakened its own security.

The reaction among industry leaders has been swift, with an increasing number bowing out of their engagements at the conference which will host Comedy Central host Stephen Colbert as a keynote speaker – as time goes on.

Josh Thomas of Atredis Partners said on December 22 that his "*moral imperative*" compelled him to cancel his scheduled talk. Chris Palmer and Adam Langely, two of the chief security experts at Google, followed suit, only to have Mikko Hyponnen do the same. Hypponen is the head research officer at F-Secure, a cybersecurity outfit based in Finland, and wrote an open letter to the heads of RSA and its parent company, EMC.

"*Eventually, NSA's random number generator was found to be flawed on purpose, in effect creating a back door*," he wrote. "*You had kept on using the generator for years despite widespread speculation that NSA had backdoored it…Aptly enough, the talk I won't be delivering at RSA 2014 was titled 'Governments as Malware Authors*.'"

After that came Chris Soghoian, the principal technologist for the American Civil Liberties Union; Electronic Frontier Foundation special counsel Marcia Hoffman; Jeffrey Carr, CEO of Taia Global security consultancy; and Mozilla's global privacy and public policy leader Alex Fowler.

Carr, in a post on his blog, said that each person who chooses to reject the RSA is doing the right thing, however small their stature.

"*Granted, I'm not Mikko Hyponnen and my talk was a mere 20 minutes on the last day of the RSA conference, but I think it's vitally important that those of us who profoundly object to RSA's $10 million secret contract with the NSA do more than just tweet our outrage*," he wrote. "*We need to take action*."

End of article "Growing Number of Security Experts Boycott RSA Conference for NSA Ties"

I could go on and on regarding the dealings of RSA and the more than shady dealings with the NSA and selling out to the NSA. But I have since discovered that the RSA corporation in fact (up the ladder) has financial and controller ties to not only the NSA but to the controllers who manage the puppet federal government of the USA.

As a side note a number of years ago the owner of MicroSoft one Billy Gates had a run in with the government for anti-trust and unfair competition practices that other small businesses had been complaining about for decades but with no results. Seems Billy was playing hardball with the gov about not letting them have complete access to backdoors into MircoSoft products used in business and personal computing around the world. It seems that all the charges magically were dropped when Billy caved and then you saw Billy hanging with the new world order world banker mid-level managers. He even got to buy into his very own large scale telescope mostly completed in South America with other funding that had apparently dried up. Yes Billy got to come in and finish this with his now safe money and status. All kinds of wonderful benefits happen to you when you sell out your fellow citizens to the NSA. If you don't believe me ask the super wealthy prior owners of Google, Facebook, and other social media that now are used to snoop on the public. .

IX. FAQs (Frequently Asked Questions)

This chapter could be very long but I have limited to a few fundamental questions that most people would like to know. Just remember that we are in a complex information war. Some people would like to enter an age of no modern devices and go back to the day when food was food, a man's word was based on the shake of a hand and your house was your castle.

FAQ #1 - is there hope for the personal computer to be snooper free ? ANSWER … yes … you have to simply lock your computer at a certain level with no new updates and no connection to the internet. You would then use another computer to access the internet for mail and other functions like browsing and only move information from the locked computer to the internet access computer with newly formatted (deep formatted) memory devices and never move anything from the internet access computer to the locked computer. After working in the field of secure computing, the only secure computer is one that never is connected to the internet. I would also get away completely from any MicroSoft Windows products. I have often said that there is an amazing business opportunity for a young bustling group of computer developers to develop a Windows look-alike operating system that could easily port the windows data and applications from your computer, fend off the attempts to enter backdoor hooks into your new OS (operating system) and offer a hacker virus free environment. The operating systems of today overburden the computers needlessly to perform the average functions of the average person or business.

FAQ #2 – how militant is the NSA about snooping ?

ANSWER … EXTREMELY militant … not only do they have a "job" to do but they take it with a vendetta. You are considered a criminal and terrorist and all are suspect. But remember they are not protecting you against terrorists (foreign or domestic), their real job is to squelch any public uprising that would target the bankers and their middle management governments that populate and control the populations of the globe with phony economies, wars, taxation and interest on fictitious fiat money. The bankers take this very seriously and have killed everyone including presidents so do not think you are somehow special and above their snooping eyes. Paranoid people many times have a reason to be paranoid and at the top of that list are the nameless bankers that have held the world in slavery for the past many hundreds of years.

FAQ #3 – will the current book on breaking RSA have an effect on protecting the public from the NSA snooping activities ?

My goal is to break this topic and understand that it is a super small David fighting a colossus Goliath. It hopefully will breach the subject that encryption codes are NOT SACRED and all of them can be broken. There is still a good deal of use of the RSA encryption "keys" that are in government and military hardware and software that no one even knows about. They were programmed into machines and chips and software and the design work never really kept track of it since this type of computer programming is all compartmentalized and since no one ever imagined that someone could break these codes not much attention was paid to the issue at the time. Additionally to catalogue and list where the codes were could be lost or fall into the wrong hands so literally almost all of the use of the prime number encryption codes are lost in cyberspace but still exist.

But the bigger issue is an educational tool for the public. Very few people have the ability to use this text along with the original text Calculate Primes along with all the other information you would have to use to hack into secure government or corporate facilities and if these entities have not build front end and enveloping capacity around their systems to protect them then shame on them. They should all thank me for exposing this issue rather than finding out someday that the secret lay hidden somewhere and only released after extensive damage was done. The real issue is that the public can now see and understand the extremely complex world of computer security and how it affects their lives, and additionally to see the levels of corruption by men in suites who are entrusted with the highest levels of security and how they can turn it on you the public to eaves drop into everything you do including the color of your Sunday jockey shorts (literally).

FAQ #4 – will you continue to break other encryption codes ?

I have no time at this point to work on other forms of encryption code simplification. The current work happens to be an offshoot of the resolution of the oldest problem in mathematics to directly calculate prime numbers. It was never my intention to break encryption codes. It just happens to be a minor side real world application for the solution of a very esoteric mathematics problem.

.

X. Defining the Problems

We have now entered the "how to" portion of the book. This first item is to understand some basics of computer encryption.

Encryption 101

There are many ways to encrypt or translate letters and numbers so that no one else knows what your information says. In World War II entire teams of experts were hired to develop secure methods of sending information so the enemy could not intercept and understand the contents of sensitive information. Likewise entire teams, many times consisting of mathematicians, tried to break the enemy codes. Some of the greatest intrigue tales of the war involved breaking codes and intercepting vital information.

After the war the engineers and mathematicians came home and started the computer era. I personally saw this at an early age as IBM, CRAY computers, Honeywell and Control Data as well as many other companies with supporting products like 3M (which made magnetic tape and memory devices) were established and grew in my home state of Minnesota. I watched farmers' wives in my home town soldering by hand the repetitive circuit boards that made up the first supercomputers. I used punch cards to program my first computer programs. I watched these industries grow and change and worked as a physicist mathematician and engineer in the growing computer industry. I eventually was head of the computer science department at one of the universities I worked at in a foreign country and I helped write the first standardized computer test for university level students as schools began to bring computer science into their curriculums.

Throughout my career I worked for over 10 years as a Principle Engineer overseeing all aspects of computer software and hardware design. I wrote the Functional Specifications for all new products as we build IBM compatible "Front End Processors" or FEPs designed to do the secure computing for the world's largest computing facilities. Encoding and verification at all levels was paramount. We not only designed the computers but we had our own microchip design and manufacturing facility so we designed the microchips including the timing and microinstruction sets that would be used by programmers to encode the complex functions. I originally started in this company as a "Network Engineer" doing mathematical simulation and performance engineering so the machines worked within the critical timing of the communications functions.

Encryption and coding is used at literally all levels of computing, networking and protection from any outside intruders as the information is passed from memories to microprocessors to multi-cable "busses" to transmission protocol processors to the outside secure networks only then to be received by the other end or passed on to other secure computing facilities based on pre-designated algorithms. Coding and passing of secure data is found at every level of software and hardware in the computing world.

Prime Numbers - the Basis of Encryption

In 1977 a group of mathematicians developed an encryption method called the "public key cryptography system" which used the accepted fact (at the time) that large numbers with just two prime factors of about the same size would be impossible for anyone to break the "key". They worked like this. At great computing effort the public "key" number was derived which was the product of two large prime numbers of about the same size (this added requirement will be explained in a minute). Anyone could use the public "key" to send data by an encryption algorithm BUT the receiver of the information needed the two prime number factors (and the publically available de-encryption algorithm) to decode the information. The idea being that the factorization of the "key" would be impossible because it would take vast amounts of computer processing time and the idea was that the keys would continue to get larger and larger keeping them always out of reach of even the most powerful supercomputers and certainly the average Joe on the street.

At the time and before my Calculate Primes book was released, the only way to factor large numbers was to literally start by dividing the number by all of the prime numbers starting with 2, 3, 5, 7, 11, 13 and on and on until the factorization was complete. Given this method if one of the key factors was small then you would arrive at the factorization solution faster than if the two factors were about the same size. Thus the "RSA" codes as they commonly became known had mathematicians calculating the amount of currently available supercomputer time to solve the problem.

All was well in computer encryption land and a boastful "RSA Challenge" was posted on the RSA home page listing available large public "keys" with a prize monetary amount for anyone that could break these factorization problems (see Chapter XVI for details). Some of the prizes offered significant rewards for anyone to resolve the factors. As previously noted the RSA Challenge prizes were removed from the internet shortly after my book Calculate Primes was released.

As one commenter stated when asked about the public "key" encryption method, "It is a fact that we don't know how to efficiently factor a large number. That gives cryptographic algorithms their strength. If, one day, someone figures out how to do it, all the cryptographic algorithms we currently use will become obsolete."

The cover of this book shows a single 617 digit decimal number that translated into its base 2 binary number equivalent is 2048 bits (0's and 1's of computer binary code). Thus comes the term "2048 bit encryption". You possibly have heard the more common terms such as 128 bit encryption or its big brother 256 bit encryption. This refers to the number of binary bits in the public key number. Typically for reasons already given the factors will have about half that number of digits in each prime factor. This is a benefit in making it harder to factor a number by a brute force supercomputer algorithm, BUT as you will see with the method given in this book it actually makes it extremely easy to "select" the factors and therefore break the RSA codes.

Traditional Methods of Factorization

There are advanced methods of factorization that can cut corners from the completely brute force method of dividing a number by all the prime numbers up to the square root of the number being factored. First of all if you were trying to break an RSA code you would have to divide by all the prime numbers that were approximately one half the number of digits as the main number or about the size of the square root of the number. This operation becomes increasingly difficult as the numbers get increasingly larger. Computers are not especially efficient at division and with large numbers special algorithms are needed to handle the large number of bits as computer registers in your average supercomputer are rather small compared to the large public key numbers. All of this complicates the processing and extends the methods.

Additionally you would have to develop prime number tables and these are not generally available for the size numbers we are talking about here. When computing search programs look for large prime numbers they do not search for all possible prime numbers but search for number types which have a higher probability of being prime. For example the largest know primes (see Chapter XVI for more details) are of the 2^p -1 where p is a large prime number. These are known as the Mersenne primes and offer a more fertile area to search for large prime numbers. But in the process all of the other prime numbers fall through the cracks and no one searches for them. So if you are a budding computer hacker wanna bee you not only have to have a supercomputer at your disposal, you also have to generate extensive tables of prime numbers with severe

amounts of computer crunching to get to the level you can even begin dividing them into the public key.

The end result is that as long as the RSA keys remained ahead of current supercomputing power and the intruders had no other method than brute force computing at their disposal, the keys were safe from intruders. This was all well and good until the solution to the prime numbers was presented and the dreaded day came when cracking the patterns of the primes and directly calculating primes in large groups came along.

Direct Calculation of Prime Numbers

The original text Calculate Primes discloses the heart of the solution to the oldest problem in all of mathematics … the direct calculation of the prime numbers. For those who are just interested in an overview of Breaking RSA codes simply proceed to the next section. For those interested in actually working on some of the large RSA encryption keys given on the cover and with additional numbers given in Chapter XVI you can finish this book but you will have to read and fully understand the contents of the Calculate Primes book.

In summary there are 7 parts to the solution of the mathematical puzzle to understand the direct calculation of prime numbers, but essentially you start with 0 and 1 and generate the first set of primes. You then take this first set of prime numbers, enter it into the Generator Function and repeat step 1. This generates a second and larger group of prime numbers. You then take this new set of primes and enter into the Generator Function and derive a third and much larger set of prime numbers. This process cycles again and again with each succeeding group of prime numbers getting much larger than the prior group. Within a few short iterations you have effectively identified the vast majority of prime numbers all the way to infinity.

With each iteration something very important happens relative to breaking RSA codes. The patterns of the prime numbers repeats out to infinity so at any point you can stop and the set of numbers you have left contains ALL of the prime numbers to infinity plus a few more that become eliminated with each step of the Generator Function. At any point you can select to stop generating prime numbers and concentrate on breaking RSA codes. The exact method will be described in detail in Chapter XII.

Other Types of Encryption

Other types of encryption include what are known as “elliptical” algorithms, others use random number generators or other “one way” functions which are easy to process in one direction but difficult to resolve in the reverse direction. The point in all of these is somewhat the same as the public key method using prime numbers. Going one way mathematically is easy but going the other way is difficult and would take more computing time than is practically available.

The Long Term Effects

The issue of secure computing is a moving target for both the defender and the offender (the hacker). There are many cases of little Johny sitting in his basement discovered playing war games on the Pentagon computing system or teams of foreign hackers waging cyber attacks on US companies and government or military installations.

The passage of legislation can have no effect on the reality of secure computing. Teams of specialists work very hard at this huge issue that is as volatile as any security issue we face. There is a secure computing “Czar” resident in Homeland Security whose job it is to oversee the daily defense of our country. This will go on for as long as there are computers and enemies or even people looking for a fun computer experience. The issue with the public is that the government now is spying on everything you do and you are currently left defenseless as computer software and hardware companies fold to government (NSA) demands to provide back doors into your computer, call phone, television, smart electric meter on the side of your house, etc. etc. etc..

Part of the ruse is to keep the public convinced that 128 bit or the allegedly more powerful 256 bit encryption is secure. It is like in the Middle Ages when the Kings and Queens and “secret societies” knew that the world was not flat but convinced the public by simply repeating the mantra. For hundreds of years this kept any young ambitious adventurers mentally enslaved because why would you build a ship and sail away for riches and fame when you would just fall off the end of the world? The same is true of secure computing. People buy “mal-ware” that has no more protection than the man in the moon. They are full of backdoors deemed necessary by the gov agencies to keep you completely under surveillance, while TV shows and Hollywood movies are used to quote the secure level security offered by “256 bit” encryption. The same backdoors are well known by hackers and leaves the doors wide open.

XI. Hilbert's and the Millennium Problems

THIS IS A VERY IMPORTANT CHAPTER … we are almost to the heart of the book to break the RSA codes but please be patient as you read this chapter … it is extremely important in understanding the history of this entire issue.

Although this is an extremely esoteric and remote topic for the average man on the street and even for most high level physicists, mathematicians and engineers, the correct understanding of the top unsolved problems in mathematics can shed some light on the current topic of breaking RSA encryption codes. The topic at hand is completely immersed in serious levels of mathematics, which allow predictable security for a given encryption system including the use of prime numbers as factors of large numbers … the system adopted by RSA Laboratories (no they did not invent it they just adapted it and with large supercomputing facilities capitalized on existing knowledge).

First you have to understand a little historical background. Throughout history mathematics has seen many revolutionary developments too lengthy a list to quote here, and with an equally impressive list of mathematicians who opened doors and gave understanding. Many of these worked alone while cracking some of the hardest problems in the field which then gave way to decades if not centuries of further work. Amongst all of this has ALWAYS been the search for a deep understanding of the prime numbers. At the time of the release of my Calculate Primes work the best that the top mathematicians in the field could say about prime numbers is that "they looked like a random set of lottery numbers".

Literally every great mathematician, physicist and many others have tried in vain to make the least amount of progress. Einstein who gave some of the most subtle and innovative directions in mathematics, statistics and physics failed to make a dent in the prime number problem. Prime numbers are the basis of all numbers. One of the most fundamental proofs tells us that all numbers have a unique set of prime factors. Prime numbers are defined in terms of this theorem in that they are the unique numbers that have only themselves and 1 as factors (they have no other factors). A main mathematical analysis result regarding the "density of primes" or the occurrence of primes along the number line is expressed in terms of natural logarithms BUT it does not resolve the issues such as the simple question … if we go far enough on the number line will there all of a sudden be large clumps of primes and where will these occur? Mathematical analysis cannot answer even the most rudimentary of questions yet it has been the only "tool" in vogue for over 200 years. My

work radically changed all of that but the mathematical world remains in their ivory towers hoping somehow that generalities of Mathematical Analysis will resolve their misunderstanding of the prime numbers.

As mentioned before throughout modern mathematical history the use of base 10 numbers has defined everything including important physical constants such as π and e (the base of natural logarithms) as well as other countless physical constants. The problem that I discovered in resolving the prime number problem was that the base 10 number system was not the solution but it in fact was a great part of the problem. Large decimal numbers had no ability to define prime numbers. They were simply long strings of meaningless digits.

What my work did was both redefine prime numbers and the number relationships. Instead of 1, 10, 100, 1000, etc., I redefined the numbers in terms of what I called the "magic numbers" (a term used for the general public in the book Calculate Primes). In mathematical terms these are called "Sequential Prime Products". Although they had been used to some degree in mathematics and even the great Gauss tried to use various base number systems to study the prime numbers, no one recognized that the prime numbers were symmetrical around these base numbers until my ground breaking work on prime numbers. So instead of the base 10 system, my new system was as follows … 1, 2, 6, 30, 210, 2310, 30030, 510510, etc.. These happen to be the numbers that are products of all the prime numbers up to a certain point.

This system of numbers grows much more rapidly than the base 10 number system and this gives rise to directly calculating very large prime numbers very rapidly. The prime numbers had symmetry, reciprocity and closure which are very important mathematical concepts. Additionally the system developed what I called "false primes" (in mathematical terms these are relative primes to a specific group of numbers). These false primes were used in the generation process and once their usefulness had ended they were discarded by the natural process of directly calculating the prime numbers. The prime numbers had families with ancestors and decedents and were not calculated just one at a time. This also gives rise to the rapid calculation of very large bodies of prime numbers with the ability to predict much larger prime numbers (also in large groups). Additionally what we used to call factorization was now replaced with a simple addition or subtraction test of a number relative to the "magic numbers". And lastly, it did away with the base 10 number system.

All of this makes it possible to rapidly break the RSA codes as you will see in the next Chapter, but first a bit of history regarding Hilbert's and the Millennium Problems.

In 1900 mathematician David Hilbert gave a famous speech in Paris outlining the 24 unsolved problems that would shape the world of

mathematics over the next 100 years. Number 8 on the list but first on the minds of all mathematicians was a long standing problem called The Riemann Hypothesis. Alongside this he listed other problems related to prime numbers. Rather than directly state that there was no solution to the prime number problem dilemma he listed The Riemann Hypothesis … and this is the important part … that was deemed to be the only hope for unlocking the key to understanding the prime numbers. The basic equation was long before formulated by Euler and adopted in a form using complex numbers by Riemann. On one side of the equation was a complex mathematical formula involving prime numbers in an infinite product whereas the other side of the equation involved all the integers in a similarly but less complicated formula combined in an infinite sum. This was called the "Golden Key" as it related prime numbers to the counting integers.

It was believed that if someone could solve this complex equation and relate the primes to the integers that it would in turn shed some light on the nature and order of the prime numbers. To date it remains unsolved and is considered the very top unsolved problem in all of mathematics.

The real issue is that Hilbert and all of mathematics were desperately searching for a solution to the rhythm and understanding of the prime numbers. Hilbert was quoted as saying that if he were to sleep for 1000 years and he woke up his first question would be "has anyone solved the Riemann Hypothesis". This led to the concept that the prime numbers were "safe" from direct calculation and therefore were a good bet for the public key encryption methods that were employed by the RSA Laboratories in their marketing of secure computing algorithms.

At the turn of the 21st century in the year 2000 a group called "The Clay Mathematics Institute" formulated 7 of the top unsolved problems in mathematics which they called "The Millennium Prize Problems" and top on its list was once again The Riemann Hypothesis. This indicated that no progress had been made regarding the prime numbers. Other lists of unsolved problems included the same problems Hilbert had listed along side of the Riemann hypothesis 100 years earlier. Literally none of these problems were any closer to being solved in the year 2000. All remain unsolved at the time of this writing.

In 2008 DARPA as the cutting edge research agency for the Department of Defense in the USA designated 23 problems that if solved would give great advancements to their ability to create defense for our complex military needs. In its list was the proposal to solve (or disprove) the Riemann Hypothesis. In the needs of DARPA the obvious connection was to understand prime numbers to bolster secure computing algorithms using prime numbers which was central to literally everything they did.

When I solved the prime number problem I neither used The Riemann Hypothesis nor any other math analysis techniques that were in common use. I knew there had to be a completely different approach and my research indeed paid off. The solution was staring everyone in the face and in retrospect many of the great mathematicians had played around with some ideas but never broke through the barrier to understand the true nature of prime numbers. I discuss my discovery in the Calculate Primes book.

The Riemann hypothesis remains the great Holy Grail of Number Theory. Yet if my work on prime numbers had existed prior to Hilbert's speech in 1900, The Riemann Hypothesis would probably never have been included in Hilbert's list. The entire reason it has been listed at the top of all mathematics problems for hundreds of years is because it was deemed the only known hope for cracking the understanding of the prime numbers. As new prime numbers are determined by brute force computing methods, they are plugged into the Riemann Zeta Equation and all to date fit the designated hypothesis that all of the Riemann "zeros" lie along the real ½ line on the complex plane. But no one is even sure that if someone resolves this Holy Grail problem, it really will offer a hope of understanding prime numbers.

Many people try to measure the success of my work relative to "solving the Riemann Hypothesis" or calculating larger than already discovered prime numbers or breaking the RSA -2048 public key. Understand that NONE of these are legitimate claims since the Generator Function, which is the basis for the understanding of prime numbers and the core of the Calculate Primes work sidesteps all of these issues. The Riemann Hypothesis becomes a non-issue because now there is a completely different method to understanding prime numbers which no one imagined before. That is the measure of greatness of new discoveries, not that they follow the imagined patterns of yester year. Regarding the largest prime numbers, remember that the supercomputing algorithms calculate specific types of prime numbers and leave the rest (the vast majority) unexamined, but on an apples to apples basis, yes the Generator Function has far more power than just calculating a single large prime number. Remember that the prize organizations do not allow the McCanney Generator Function to be used to claim their prizes and closely monitor contestants to use only the specified computer algorithm that they specify. They are stuck on the gee whiz idea that super computers need to be used to calculate large prime numbers. The McCanney Generator Function gives understanding to the prime numbers; brute force calculations do not and tell you NOTHING about where the next one might be; the Generator Function does this all the way to infinity. And regarding the RSA -2048 or any other public "key numbers, the fact that

the RSA Laboratories revoked their prize money offerings weeks after my Calculate Primes book was released should tell you the story on that issue. My tables of solutions of these public keys are for sale, not for free publication on web pages or blogs.

But if you are a real student of mathematics, the real issues are far deeper. I would add to this list the ability to do a better job at understanding as with subtle issues such as the "density of primes" that currently is "bounded" by an equation using logarithms. The standard equation that has been used literally for centuries (and not improved upon) depends on the idea that prime numbers become fewer and fewer as you get farther and farther along the number line. HOWEVER, it tells nothing of individual prime numbers and cannot answer even the simplest question such as localized groupings of primes as you get far out into very large numbers. Using Mathematical Analysis very little can be said that is concrete about any specific regions of the prime numbers. To the contrary the Generator Function defines ALL of the number line and predicts exactly where all the concentrations of prime numbers will be as you move out to infinity.

This is because now prime numbers are understood to be generated in "waves", where waves of prime numbers within the "wavelength" of the centrally important "magic numbers" modify each set of previous waves and therefore you see the prime numbers being built in patterns all the way to infinity. The Generator Function provides not only a measure of the density of prime numbers but it also guarantees that there will be no unexpected large clumps of them somewhere way out there. Every iteration of the Generator Function provides a set of primes modified from the last set and is monotonically decreasing (a mathematical term for constantly decreasing without ever increasing). Not only does it define the density of primes but you can see the so called "unexpected clumping" of primes and understand why this is occurring in terms of waves of numbers rather than a simple logarithmic function that provides no meaning to any individual or group of primes as you proceed out to infinity.

This is all explained in detail in the original text Calculate Primes but it is important in light of the current text not to get caught up in the ivory tower myopic view of calculating the largest prime number or the resolution of the Riemann Hypothesis or the really ridiculous and out-dated referral to breaking RSA public key encryption codes that were broken years ago, but for which RSA Laboratories and the lying government agencies are still trying to keep the public from knowing about since it is still used to pretend that the public has cyber protection when it very much does not.

Some have wondered why I do not publish this material in the so called "peer review" journals. The reality is that 99% of all real research

in science, engineering and mathematics, which includes the vast majority of real advancements, ARE NOT published in peer reviewed journals. Einstein never published in peer review journals and distained them (especially in the USA) for their snobbery and misuse of the system to monopolize various fields (his two peer reviewed papers were published before he came to the USA). Most fields of study and the peer review journals that cater to them are harbored by small groups of ivory towered snobs who use peer review to keep themselves in their vested positions and to keep others out. This by the way is the main problem with the Clay Millennium Problems prizes is that they require that one publish the results in a peer reviewed journal to claim the $1 Million prize. The author would have to give up all rights to their research to claim a seemingly large but in actuality miniscule prize, given the magnitude of the solution.

I personally have a number of early career peer reviewed publications in astrophysics and space science journals however I have refused to submit to this system for the same reasons. Additionally the journals become owners of the work and the author needs permission to quote his own work. Excuse me, but this is one more element of the "publish or perish" syndrome in universities which removes all ownership from the laborers and puts it into the hands of the world controllers. Why would I give my lifelong hard work to them? There are too many cases where anonymous journal referees have buried papers in their field only to surface with the material at a later date. I personally was a victim of this while at Cornell University. I want nothing to do with any of this.

One of my pet subjects is the ownership of science. Scientists have completely lost control of their work and what it is used for, and in the case of all the work done on encryption and computer security, you can now see that it is being used against the public. The scientists do not own their own science. The public who paid for this does not own it either. So who owns science and scientific advancements? Simply put, the world bankers who fund the governments of the world own it lock stock and barrel and they use it for whatever means they see fit. Scientists, engineers, mathematicians, high tech corporations, governments, their militaries, world resources and last but certainly not least you in the general public are all just pawns in a large monopoly game of control and deceit in the age old system of central banking. Today at the core of all of this is the cyber maze and secure computing.

.

XII. Breaking RSA Codes

Breaking the RSA public encryption keys amounts to rapidly finding the two prime factors of large numbers. Chapter XVI gives a long list of such numbers … some resolved and some yet to be solved. All have been designed by the RSA Laboratories supercomputers. So they have the solutions on record. Each unsolved number had a cash prize associated with it based on the perceived difficulty of the solution. These prize awards were removed a few weeks after the release on March 5, 2007 of my book Calculate Primes.

The text below will take you first through some rudimentary methods of breaking the codes and after these are presented a tutorial will give advanced methods that will speed up the process greatly including the use of parallel processing. In many cases parallel processing is hindered by the fact that the process at hand alters the data base and therefore other steps cannot be performed even though parallel computing power is available. The case of using the Generator Function and locating the public "key" factors does not have this drawback so any level of parallel processing can be used. In cases where serious efforts are made there is no limit to the use of parallel processing that can be employed.

No Body Ever Thought It Would Be Done

In designing the public keys (the large number with just two prime factors) the keys were intentionally chosen so that the prime factors would be approximately the same size. This was done because in the world of supercomputer factorization any search would start with smaller numbers and work up to larger numbers to test (by brute force division) if a candidate prime number was a factor or not. So if one were to choose one smaller prime number and one larger prime number, the computer search would arrive at the smaller number in less time and solve the problem … thus the selection of two prime factors that were of about the same magnitude.

Take the resolved public key number

RSA-100 has 100 decimal digits (330 bits). Its factorization was announced on April 1, 1991 by Arjen K. Lenstra.[3][4] Reportedly, the factorization took a few days using the multiple-polynomial quadratic sieve algorithm on a MasPar parallel computer.[5]

The value and factorization of RSA-100 are as follows:

```
RSA-100 =
1522605027922533360535618378132637429718068114961 3

8068865790849458012296325895289765400035069200613 9

RSA-100 factors =
3797522793694367392280887275544562785456553663819 9
        ×
4009469095092088103068373529276146838921489972406 1
```

Note that the RSA – 100 number has 100 digits whereas the factors each have 50 digits. But just as an exercise now that we know the factors, let's multiply them together to get the larger RSA 100 number. Take this as an exercise and write the two factors one above the other, you may wish to use graph paper to keep the numbers in rows and columns. Start by multiplying the first two right hand digits. 1 x 9 = 9 (write the 9 down and there is nothing to carry to the 10s column). Note that the last digit in the RSA -100 number is "9". This is standard second grade manual arithmetic multiplication. When you complete this row of multiplying 1 by all digits in the top factor you place a "0" in the right hand most space of the second line of your multiplication solution and continue multiplying the next right most digit "6" but the first product 6 x 9 = 54 you place the 4 and carry the 5 … and then continue multiplying the rest of the top number by 6. Note that all the digits multiplied to the left do not contribute to the lower order final product digits. Only the lower order factor digits contribute to the public key RSA 100 lower order digits.

The point is that the digits of the product starting from the right hand side 9, 3, 1, 6 etc. are predictable based on the two factors' right hand or lower order digits. This is one of the fundamental concepts needed to quickly break the RSA codes as you will see.

Secondly now look at the higher order digits of the two factors. But first for simplicity let's put the two factors into decimal formats. The first number becomes 3.797522… x 10^{49} whereas the second factor has the form 4.009469… x 10^{49}. Now multiply these two base numbers together but just the 7 digits that I have listed (forget about all the other digits for now and also forget for the moment the 10^{49}). Using a hand calculator you get 3.797522 x 4.009469 = 15.226046 … now compare this to the left most digits of the main key RSA 100 number. Surprised ? Except for a small factor in the last two digits (46 vs. 50) you have exactly the number AND WITHOUT MULTIPLYING ALL THE DIGITS.

Now what if you had a large table of prime numbers from which to select potential factors containing all the prime numbers in the region of

interest (numbers with about 50 digits) and all you had to do was pick the factors and match them up from your list.

Let's review the selection aspects of the process. Recall that you are given a large number with a designated set of digits (in the example above the number has 100 digits or 330 bits … this is called "330 bit encryption"). You know that RSA Laboratories pick the numbers which have factors to be about the same size because their mathematical statisticians tell them this creates the hardest factoring problem for hackers who they expect would be using the most powerful computers at their disposal and additionally would be using what they think is the only way to arrive at those factors … brute force calculations.

But you now have the power of the Generator Function at your disposal to generate large tables of prime numbers relatively quickly and in the region of the number line of interest. Your selection process has a number of tests that you can use to quickly eliminate the lists of potential prime factors WITHOUT EVER PERFORMING LARGE NUMERICAL DIVISION OR THE LENGTHY PROCESS OF BRUTE FORCE FACTORIZATION.

Once again the tests, which can be made simultaneously on an average sized computer are listed below. First select numbers in sequence from your list of potential prime candidates that you have generated using the Generator Function and then select the second number also from the same list. These are potential factors of your public key number. Using the following tests simultaneously you can eliminate the pair as a possible pair of factors for the public key RSA number and eventually locate the pair of prime factors that are in fact the correct pair that multiply to equal the public "key".

- Magnitude test of the two factors – will the product of the two numbers of the given magnitudes produce a product of the required size for the public "key"?
- Lower order digit multiplication test – multiply the lower order digits and compare to the lower order digits of the larger number. If the first digit matches then multiply further to get the second order lower digit. NOTE you do not have to multiply the entire number to get the lower order digits (just the first lower order digits) in fact for the second order digit you only have to complete the second digit product of the lower order digits of the two potential factors. If these match the lower order digits of the public "key" then determine the third order lower digits. You will find that MOST numbers that are not a true match are eliminated within at most the first two or three iterations of the lower order digit test. If you get past the 4^{th} or 5^{th}

lower order digit you most likely have a match and can continue multiplying.

- Higher order digit multiplication test – as done above take the upper 7 digits of both potential factors and multiply them to see if they match the upper most digits of the public key number. They should be exact to the first 5 or 6 digits. If not the test fails and go to the next set of potential prime factors.
- Perform these tests simultaneously and if any test is negated exit the other tests immediately and go to the next set of prime candidate numbers from your table

You can see that the entire process is very different from the brute force computer division test. It depends on your ability to quickly select and calculate large tables of prime numbers in the region of interest without having to calculate all the prime numbers although real hackers would certainly have this accomplished and have their extensive tables on line during the hacking process.

The Generator Function

I am not going to review the Generator Function in this book. The serious student intent on breaking RSA public key encryption codes needs to read and understand that book. Many people have done this so it is not beyond the scope of the average computer literate person. One suggestion is that you do not have to generate all of the prime number tables. You will learn that you can generate large tables of primes based on initial iterations of the Generator Function which will have what I call “false primes” and if you follow the repetitive patterns of the Generator Function out to infinity the patterns repeat. Be assured that ALL PRIME numbers are contained in the repetitive list out to infinity BUT there will be actually some of them that are what we call “false primes”. For example if you generate the prime numbers including the “false primes” for the “magic number” 510510, you will have secured all the real primes out to the square root of this number or just 714. However, if you look at the repetitive “wave” that extends to infinity based on the number 510510 (the wave repeats to infinity with length 510510) you can be assured that all of the prime numbers are contained in the list to infinity along with some extra “false primes”. The point is that in the elimination process noted above using the tests these false primes will be eliminated very quickly and thus do not pose a problem. So you can now go to the region of interest and produce a list of all the prime numbers in a given region without generating all the prime numbers up to that point.

If you have limited computing power you would be better off computing a smaller prime number table (using a smaller magic number) and extending the pattern out to your region of interest based on the Generator Function (in the above example to numbers with 50 digits) and to weather the extra false primes in your elimination process than to attempt to calculate an exact prime number table all the way out to numbers with 50 digits. The serious hacker will take the time to generate extensive exact tables as this will allow him or her to skip from one public "key" to another rapidly.

Factorization vs. Factor Searches

The end result comes down to the fact that you are not trying to perform computer intensive factorization but are generating a list of prime number factor "candidates" in the region based on the knowledge that the factors are going to be about the same size. Do you see now how this strategy used by RSA and the encryption industry and theoretical work plays into the new technique of using the Generator Function to quickly generate large tables of prime numbers just in the region where you need them and then eliminating them one by one with very simple tests which only require small multiplication of a few digits of the potential candidates chosen in sequence from the table.

Additionally the tables do not have to be "perfect". Generating complete prime number tables is not really productive use of your computing time. It is more a personal choice and requires a tradeoff. You can either generate extensive prime number tables that are exact which will make the factor selection process easier OR you can save time by creating smaller prime number tables and extend them to infinity using the wave like nature of the prime numbers as explained in the Calculate Primes book and spend a bit more time running the number tests described above because your lists will contain some "false primes" that will slow your process in the testing phase. There is no magic formula to tell you which method is better.

Now for some advanced techniques. Many astute students of this topic may already have figured out that the tests above are not the fastest way to break the "keys". Take the example of RSA – 100 with 100 base 10 digits and with factors of 50 digits each. Of course in breaking an unknown code you do not know that the factors will have 50 digits each but you are pretty sure there will be nearly 50 in one factor and a corresponding magnitude in the pair factor so that their product will have 100 digits. As you select numbers from your prime number table to "test" it is far easier and faster to take the first few higher and lower order digits of the "key" number and the first few higher and lower order digits of your test number

taken from your Generator Function table and quickly generate the digits that have to be the higher and lower digits of the second factor. Next you search your table for numbers with these higher and lower order digits. In this simplified process you do a "compare" of the second factors for the higher and lower order numbers testing each number of approximately the correct magnitude. The "compare" instruction in a computer is a one cycle step and is extremely fast. So once you have determined what the higher and lower order digits have to be in the second prime factor (based on the selection of your test number from the Generator Function table) all you have to do is perform the three tests simultaneously. These are 1) the higher order digits test compare; 2) the lower order digits test compare and 3) the magnitude test which is the same as the original set of tests to verify that the product of the two factors would result in a number of the correct magnitude.

This set of tests is subject not only to large scale parallel computing but also to what is known in the computer industry as "pipelined" instructions. One process is performed before the other two processes and this eliminates or verifies a given number based on one test (the least likely to succeed) so you do not have to waist computer cycles performing all the tests except for the ones that hold the promise that all three tests are "true". This further speeds the process.

What is somewhat humorous (but not for the users of the public key RSA encryption codes) is that it does not matter how large they make their codes. It is just as easy to break a code of 2048 bit length as 128 bits because you never perform full length division of the numbers but just the few higher and lower order bits. With parallel and pipelined processing sampling many thousands of numbers at a time, this process moves very quickly and is within the scope of anyone with normal computing power if properly programmed.

Remember that if you are serious about cracking the RSA numbers given in Chapter XVI please be sure to mail your solutions (certified with signature required) to the RSA corporation and tell them you used the Professor James McCanney work in the book Calculate Primes and this book Breaking RSA Codes for Fun and Profit. Don't expect a Christmas card from them. Remember that officially according to the RSA corporation and to the disinformation "open" encyclopedia Wikipedia, James McCanney does not exist.

Another possibility for making a profit for breaking the public keys is to sell them on the black market since the RSA Laboratories will not give you a dime. Even with the old RSA codes I always used to laugh at the miniscule size of their "Challenge" prize offerings when they were still being offered … $200,000 ??? they must not have been very confident in their own encryption system. I would have thought that with all the

boasting going on they would have at least offered a million dollars or more, especially since they were selling these for LOTS more than this to governments and military not to mention private corporations telling them they were safe with this level of encryption.

Is breaking RSA public keys and selling them on the black market illegal? Why would it be, you are just providing a service just like the RSA Laboratories. As I have said, if your secure computing world lives by encryption then it will die by encryption because somewhere someone is going to break your code no matter what amazing new system you invent. It is as simple as that.

Are there ways to protect computers and cyber information? The answer is YES. But using encryption is not the answer. It is like putting a screen door on your house to keep the bugs out. It will keep most bugs out but there will always be some that get in and bite you. There are ways to secure computing and as I have said earlier that is what I did for a good portion of my career, but I have no interest in working with corporations nor the government who clearly have no ethics when it comes to technology.

.

XIII. SNOOPING ON THE SNOOPERS

"It is not the strongest of the species that survives, nor the most intelligent. It is the one that is most adaptable to change."
……Charles Darwin

Darwin's statement can be adopted to be most appropriate for the secure computing industry. When the US military, the government and last but not least the RSA Laboratories discovered the release of my original book Calculate Primes, there was an immediate move to change from prime number encryption to other forms of encryption. I personally received a good deal of feedback as this work proceeded. The RSA Challenge prizes were removed from the RSA web page and other prizes such as the ones for calculating the largest prime numbers changed their rules to prohibit my methods from being used.

Encryption is a moving target and only the adaptable will survive as the hackers become more adept at breaking through the fiber of cyber security. But this opens the door for people to begin to fight back … that is … snooping on the snoopers. It also gives people the hope that they can combat the onslaught of snoopers with many techniques including items as simple as changing from MicroSoft Windows operating systems (OS). But do not listen to too many claims since everything out there has been infiltrated. If it is not subject to infiltration by the NSA then it is brutally crushed into submission or crushed out of existence.

We are in an information war and the public has already lost. Large corporations are similarly at the mercy of the NSA as they cut back door deals with unscrupulous companies like RSA Laboratories.

Where all of this will end only the future will tell but one has to simply ask if we really are that intelligent a species?

XIV. Summary

For many people this was their first good look into the complex world of computer security. This is just the tip of the ice berg. There are no easy answers and the questions many times are not even well defined. One is shooting at a complex moving target. The only real secure computing facility is one in which the computer is not even connected to a transmission line or the internet. Even then one has to guard against internal hackers and subversive agents. Ultimately it comes down to the fact that the human race is not very advanced. It is a group of children playing with matches and gasoline.

Some would attribute this to what we call "the Banker's World" in which strife and conflict are imposed on the world. Wars, taxation, conflict, interest on fiat money and unlimited use of natural resources owned by a few and processed to drive economies that are out of control. At the center of all of this strife is the computer age.

Recent announcements show that the human "chip" is being installed in people that will allow complete remote monitoring of the recipients, and a long list of government efforts to force them on everyone. All for your security and well being we are told. Each chip has encrypted information that only the overlords have access to see. What if we can enter into the "chip" network and jam it. This may be the only recourse the public has to defend itself against tyrannical overlords and governments. This book is a small beginning that hopefully will grow and be the beginning of public understanding of this more than complex topic.

.

XV. Table of Contents to CALCULATE PRIMES

XVI. Other Readings and Information

The following chapter includes other readings and information pertinent to the history of the topic of Breaking RSA Codes.

Original Show Notes for the Coast to Coast AM book release of the main text Calculate Primes

Prior to every major interview I comprise a summary and list of topics and questions to cover in the presentation. This of course helps the host and myself form a dialogue on extremely complex topics like the release of the Calculate Primes book with the included 3 hour DVD lecture. Most people rarely see this side of radio broadcasting and have no idea what goes into a major book release. After years of interviews with a talk show host you develop a certain pace and understanding of when to talk and when to let the host speak. The following is the exact copy of the email used by both Coast to Coast AM host George Noory as well as radio talk show host Brad Walton (now deceased) who at the time worked for WCCO radio in Minneapolis, Minnesota. The Brad Walton interview in its entirety is linked to my web page at the following link (in MP3 format)

www.jmccanneyscience.com/CalculatePrimesBradWaltonInterviewMarch2007.mp3

Note that after this posting is the information regarding the RSA Laboratories Secret-Key Challenge prizes that were quickly removed within weeks after the public release of my book Calculate Primes. Read also the earlier Chapter V regarding the interesting circumstances for the release of this book.

SHOW NOTES for March 5, 2007 C2C show with George Noory

NOTE: the new book title will be released on this show

- - "Calculate Primes" – Book with 3 hour DVD lecture
- Coast to Coast web site is linked to www.jmccanneyscience.com

Contact information: cell - backup – emergency - xxx-xxx-xxxx

I WILL CALL IN AS SOON AS I HAVE THE LAND LINE # ON MONDAY

I ALSO HAVE TOM'S # IN CASE IT IS LATE MONDAY

Show releasing my new book – "Calculate Primes" - with 3 hour DVD lecture

I have been promoting this release for some time.

Part of the release is presenting a part of my past that the public has never seen, dealing with University level Mathematics and many decades of working in the computer telecommunications industry, especially with computer protocols and encryption codes (the codes that allow secure internet transmission and banking transactions). So first I have included below an updated "About the Author" abbreviated from the book. I would like to start with an "about the author update" and progress to the other topics below.

Updated - About the author and the new book (abbreviated version):

This new book with 3-hour DVD lecture – "Calculate Primes" -, as promised, will present to the public a rarely seen side of the author. James M. McCanney, M.S. (Physics) is known worldwide for his research, books, radio and lecture appearances dealing with the electrical nature of the cosmos. He is also a Mathematician who has solved complex problems in Physics and Mathematics, and is an expert in computer design, solid-state physics, telecommunications, encryption and computer protocols.

Professor McCanney has taught the following mathematics courses at the University level in addition to Physics, Computer Science and Astronomy; Abstract Algebra, Linear Algebra, Matrix Algebra, Probability and Statistics, Statistics for Computing, Mathematical Logic, Theory of Numbers, Calculus I, II and III, Engineering Math I and II, Advanced Topics in Geometry and Topology.

He has worked about half of his lengthy career in private industry. Much of this was accomplished in multi-lingual settings, having worked in the USA, Latin America and with high-level Russian scientists. He has presented his research at international conferences and is a regular presenter at American Geophysical Union meetings. He has also lectured at Los Alamos National Laboratories, the Air-Space/America International Air show and International Electric Propulsion conferences.

Understanding his background is important in placing the new book into perspective.

After the Cornell years (1979 to 1981) Mr. McCanney worked for over a decade in the computer industry as a Principle Systems Engineer at a major telecommunications corporation designing computer telecommunications equipment. He also took part in international electronics standards development such as ISDN, which form the basis for current high-speed Internet communications. In this capacity, he worked on teams that developed IBM compatible communications networks for some of the world's largest corporations.

In the background Mr. McCanney continued working on the illusive mathematical problem of directly calculating Prime Numbers and other problems from sub-atomic to space physics. He believed that nature has provided simple but elegant methods to solve these complex problems. He envisioned a mathematical technique that would be applied repeatedly to generate a final solution. In this respect, many unsolved problems of mathematics and quantum mechanics and even genetic molecular structures would have their solutions in these yet undiscovered mathematical techniques. His first application of this has been in deciphering the code to directly calculate prime numbers using only addition and subtraction.

The new book (written for the general public) with 3-hour DVD lecture "Calculate Primes" – is the public release of materials already released within the mathematical industry. Numerous patents, trademarks and copyrights have been registered. In "Calculate Primes" Professor McCanney presents his "Prime Generator Function", which allows anyone to calculate the prime numbers using only addition. This work resolves a 2500-year-old mathematical problem, first introduced by the ancient Greeks. Even up to the present day, mathematicians believed that the prime numbers were random … that there was no overall pattern, rhyme or reason to the prime numbers.

In – "Calculate Primes" – Professor McCanney shows that the Prime Numbers have amazing mathematical properties such as symmetry and wave-like nature, with associations relating families of prime numbers to other prime numbers. This is presented in a manner that anyone can understand (the original Mathematical Treatise is included as an appendix). The DVD lecture further clarifies the many topics.

The www.jmccanneyscience.com web page has math exercise information for tonight's show – link up now or later (is linked from Coast to Coast AM web site)

- The audience will start calculating prime numbers during the show
- First look at the listing of Prime Numbers … take a good look as they will never look the same again

---

Before starting with the Prime Numbers – There are many implications of this work that branches out to other fields of study

- The "Prime Generator Function" is a new mathematical expression that works over and over again on solutions to get to a final solution
- There are certain "false solutions" along the way to resolve the final solution
- Genetics – a perfect example of "false solutions" … there are many "false solutions" that occur before a final solution is achieved
- What do prime numbers, snowflakes, diamonds, genetics and galaxies have in common? All have a common "process" that generates these diverse patterns in nature, yet each one is uniquely different … we will see that these same elements of nature are the same on the far side of the universe … the processes are "Repeatable" and each has a "Generator Function" that describes the basic building blocks and how they form to make more complex systems
- Many physical processes follow these same patterns
- And last but not least … today Prime Numbers are determined by "brute force factorization" of large numbers by the world's largest supercomputers. Once you have found a large Prime Number, it tells you nothing about any future Prime Numbers, so you take the next odd number and begin factoring all over again. Supercomputers are reaching their limit to calculate more prime numbers

---

The 2500-year-old "Prime Number Problem" – The Ancient Greeks

- what are prime numbers? Examples … 2, 3, 5, 7, 11, 13, 17, 19, 23
- There is an infinite number of prime numbers (proven by the Greeks)

- Numbers can be represented as rows and columns of objects … the prime numbers can only be placed in one row … you do not need numbers to understand the complex nature of the prime numbers … but numbers help us visualize
- Simply put, the prime numbers are all the numbers that are not listed in the neat multiplication table … they only have 1 and themselves as factors

---

History of mathematical attempts to decipher the Prime Numbers

- the greatest mathematicians all worked on this problem
- Riemann, Euler, Gauss, etc etc.
- Why did they fail to see the solution to the Prime Numbers? (there are many subtle aspects to the solution with false leads at every turn)
- The Greatest Unsolved Problem in all of Physics and Mathematics is called "The Riemann Hypothesis" related to the density of prime numbers along the number line (e.g. how many prime numbers are there on any given region of the number line) … there is a million dollar reward for its solution. In the mid-1800's mathematicians gave up looking for any patterns to the prime numbers. Mathematicians resorted to higher levels of complex equations in attempts to understand the prime numbers. The Riemann Hypothesis came out of that work and is understood by only a handful of people. It remains one of the greatest unsolved problems of mathematics.

McCanney's History of working on the Prime Number problem

- From high school to 4 decades later
- Giving up on purpose to get a fresh start years later
- The final solution and its many parts

Patents Copyrights and Trademarks

- There has been extensive work to provide protection of the conceptual ideas, processes and terminology
- New web page for legal inquiries by professionals (no internet nutcases please)
- I am already working with private entities on uses for the new processes

---

Let's calculate some Prime Numbers

- The "Magic Numbers" – the key to the prime numbers (note the magic numbers are not prime numbers – but are they keys to generating the prime numbers)
- The first "Magic Number" (I will give it on the air) – let's calculate some prime numbers
- "false primes" needed to generate "true primes" (example is 25)
- Another "Magic Number" – calculate some more prime numbers
- Each magic number has a family of prime numbers that are used to generate the next magic number and its family of prime number
- There are infinitely many "Magic Numbers"
- The prime numbers are generated in groups, not just one at a time
- The prime numbers are symmetrically located around the magic numbers … symmetry is an unexpected property of the prime numbers … mathematicians love number systems with symmetry
- Since they prime numbers are used to generate more prime numbers, they possess the mathematical property called "closure"
- Since one group of prime numbers generates another group … the second group in reverse and be used to generate the previous group … this is the mathematical property called "reciprocity"
- The book and DVD show how to find more magic numbers and use them in calculating the prime numbers using just addition … using what I call "The Generator Function"

The Generator Function – A mathematical equation to calculate all of the prime numbers using just addition – The Generator Function may someday be called The Holy Grail of Mathematics – it is presented and explained in the book and DVD lecture "Calculate Primes" -

- It details calculating the Prime Numbers in groups
- A sequential method starting with 0 and 1 (the building blocks of numbers)
- Ancestor groups generate new "offspring" groups which it turn are used to generate future groups … these are generated in "waves" of prime numbers like waves in a pond
- An essential aspect of the Generator Function concept is that it creates intermediate or "false" solutions that are necessary steps to generate the final correct solution. This is possibly but one of the reasons why so many mathematicians have worked around the prime number problem without finding a solution, as they failed to see the total picture as presented in this book. Countless mathematicians have come to the conclusion that that Prime Numbers are random with but passing patterns. This book proves

that to be incorrect. When you finally look at the prime number table and see why every number is there and how it is related to all the other primes, with all of their "ancestors" bridging back to the numbers 0 and 1, you will understand the powerful impact this book will have on the future of mathematics.

Encryption Codes – Are they doomed?

- The secure transmissions and transactions on the internet depend on encryption methods … some of which use large Prime Numbers as their "Keys"
- Encryption is like opening a safety deposit box at the bank. The customer has a key and the bank has a key. Both keys are needed to open the box. When the customer comes into the bank they are first identified and then allowed in to open the safety deposit box. Encryption codes work the same, only using large prime numbers as the "keys".
- Now that anyone can calculate prime numbers of any size relatively quickly, what is the fallout for Internet and banking secure transactions?

Repeatability and Generator Functions of Nature

- Based on this new work with Prime Numbers, I believe that for every process in Nature there is a unique "Generator Function"
- These Generator Functions will be universal across the Universe
- Will a diamond on the far side of the Universe have the same properties as a diamond we find here on Earth?
- Will there be planets on the far side of the Universe that resemble planets and Moons of our solar system
- Will snowflakes and Galaxies on the far side of the Universe look like snowflakes and galaxies we see here?
- Will DNA build the same on the far side of the Universe as it does here?
- This leads to questions that are being asked for the first time. For example in genetics, could the makeup of the human biped be not only duplicated somewhere else in the universe, but is the norm rather than the exception based on "Generator Functions" that operate on the building blocks of life (the nucleotides that are the base of the genetic code). Could this pattern be replicated on the far side of the universe just as a diamond would appear the same in such a distant place?

- Is the human race just an intermediate (incorrect) step required to reach a more final state, which will be capable of living in the universe? Nature's way is one of evolution and rejection. The great catastrophes weed out the unsuccessful species, which then give rise to the new more successful species. If a species does not use its time and physical resources to gain peace and learn how to live in harmony with its surroundings, it will not make it without natural catastrophes eliminating it as we have seen on earth in the ancient past. Is the current human dilemma a signature of our failure to collectively control our leaders and bring us successfully into the universe OR are we doomed to fight eternal petty earth wars until Nature's Catastrophes end our plight in hopes of generating the next genetic iteration that may be successful?
- The fact that the prime number "Generator Function", and seemingly all other "Generator Functions", create "false" results that are then needed to create "true results" appears to be a subtle but essential aspect of nature itself. Understanding this also is identical to subatomic physics where heavy atomic nuclei are unstable but are required to make larger more stable atoms.

Internet Information regarding RSA Codes

The following have been mouse copied from internet sources to record at the time of this eBook release the information one would find if you searched in a standard internet search engine for "RSA Codes". These postings sometimes change with time or are removed so it is important to see the status of an internet search at the time of this release in February of 2014.

A little background is needed to put the following into perspective. The first mouse copied page is from Wikipedia the so called "free open" encyclopedia which has been taken over and "cleansed" by groups including the NSA who now not only monitors everything you do on the internet and cell phone and home computer and monitors you through chips hidden in your television set etc., etc., etc. … but also now controls what you read on the internet. Google – Wikipedia – twitter – facebook – and on and on and on are controlled and operated by various alphabet soup agencies that invade and control your privacy. You will see that Wikipedia does not mention anything about the fact that the RSA codes have been broken and this has been known about for at least 6 years and counting at the time of this eBook release (since the public release of the Calculate Primes book).

Oddly enough they also have purged any reference to the work and history of James McCanney even though you can regularly hear my voice on interviews on dozens of top rated radio shows not to mention my own weekly radio show that is heard world-wide every week. According to the misinformation encyclopedia "Wikipedia" James McCanney does not exist. So with that introduction here is the statement on wikipedia under RSA codes mouse copied without editing (it would be somewhat humorous if Wikipedia objected to my placing this here as they would have to contact a person they claim does not exist to make their complaint. Possibly now you will understand better the title of this book … "Phun with Dik and Jayn – Breaking RSA Codes for Fun and Profit". (NOTE that the cover RSA number is derived from this general public article … and all the hyper-links to sources outside of this article are preserved for the serious students of this topic).

Additionally note the timing of the cancellation and retraction of the "RSA Challenge" prize awards totaling hundreds of thousands of dollars ended in 2007 just days after the release of my Calculate Primes book to the general public. The "official reason" given is due to "the understanding of more advanced computing methods". This of course was complete non-sense since there was no sudden jump in computing power available to prize contestants nor was there any amazing advancement in the standard algorithms. In fact with the large numbers in the RSA challenge list the standard computing times were getting vastly out of range of any contestants that were working on the problem. The reality is that the attorneys for the RSA Laboratories told them that now any 3rd grader could break their codes with a small home computer using the newly released work in the Calculate Primes book.

---

wikipedia "RSA numbers" and the "RSA Challenge awards"

RSA numbers

From Wikipedia, the free encyclopedia

In mathematics, the **RSA numbers** are a set of large semiprimes (numbers with exactly two prime factors) that are part of the RSA Factoring Challenge. The challenge was to find the prime factors but it was declared inactive in 2007.[1] It was created by RSA Laboratories in March 1991 to encourage research into computational number theory and the practical difficulty of factoring large integers.

RSA Laboratories published a number of semiprimes with 100 to 617 decimal digits. Cash prizes of varying size were offered for factorization

of some of them. The smallest RSA number was factored in a few days. Most of the numbers have still not been factored and many of them are expected to remain unfactored for many years to come. As of September 2013, 18 of the 54 listed numbers have been factored: the 17 smallest from RSA-100 to RSA-704, plus RSA-768.

The RSA challenge officially ended in 2007 but people are still attempting to find the factorizations. According to RSA Laboratories, "Now that the industry has a considerably more advanced understanding of the cryptanalytic strength of common symmetric-key and public-key algorithms, these challenges are no longer active."[2] Some of the smaller prizes had been awarded at the time. The remaining prizes were retracted.

The first RSA numbers generated, from RSA-100 to RSA-500, were labeled according to their number of decimal digits. Later, beginning with RSA-576, binary digits are counted instead. An exception to this is RSA-617, which was created prior to the change in the numbering scheme. The numbers are listed in increasing order below.

Contents

RSA-100

RSA-100 has 100 decimal digits (330 bits). Its factorization was announced on April 1, 1991 by Arjen K. Lenstra.[3][4] Reportedly, the

factorization took a few days using the multiple-polynomial quadratic sieve algorithm on a MasPar parallel computer.[5]

The value and factorization of RSA-100 are as follows:

```
RSA-100 =
152260502792253336053561837813263742971806811496138068865790849458012296325895289765400035069200613937975227936943673922808872755445627854565536638199
        ×
400946909509208810306837352927614683892148997240613579423417972586877499180783256845540300377802422822619353290819048467025236467741151351611120450406031756866735329081904846702523646774115135161112045040603175686675
```

It takes four hours to repeat this factorization using the program Msieve on a 2200 MHz Athlon 64 processor.

RSA-110

RSA-110 has 110 decimal digits (364 bits), and was factored in April 1992 by Arjen K. Lenstra and Mark S. Manasse in approximately one month.[5]

The value and factorization are as follows:

```
RSA-110 =
35794234179725868774991807832568455403003778024228226196122421090493547576937037317561418841225758554253106999
        ×
58464182144061546788365531829791623841986105056010623335324
```

RSA-120

RSA-120 has 120 decimal digits (397 bits), and was factored in June 1993 by Thomas Denny, Bruce Dodson, Arjen K. Lenstra, and Mark S. Manasse.[6] The computation took under three months of actual computer time.

The value and factorization are as follows:

```
RSA-120 =
227010481295437363334259960947493668895875336466084780038173258247009162675779735389791151574049166747880487470296548479
```

```
RSA-120 =
3274145556934980157511463037491414880636424032401714634068
3
        ×
6933426671108301811973254018997006413619658631273366806730
13
```

RSA-129

RSA-129, having 129 decimal digits (426 bits), was not part of the 1991 RSA Factoring Challenge, but rather related to Martin Gardner's column in the August 1977 issue of *Scientific American*.[7]

RSA-129 was factored in April 1994 by a team led by Derek Atkins, Michael Graff, Arjen K. Lenstra and Paul Leyland, using approximately 1600 computers[8] from around 600 volunteers connected over the Internet.[9] A US$100 token prize was awarded by RSA Security for the factorization, which was donated to the Free Software Foundation.

The value and factorization are as follows:

```
RSA-129 =
1143816257578888676692357799761466120102182967212423625625
6184293

5706935245733897830597123563958705058989075147599290026879
543541

RSA-129 =
3490529510847650949147849619903898133417764638493387843990
820577
        ×
3276913299326670954996198819083446141317764296799294253979
8288533
```

The factorization was found using the Multiple Polynomial Quadratic Sieve algorithm.

The factoring challenge included a message encrypted with RSA-129. When decrypted using the factorization the message was revealed to be "The Magic Words are Squeamish Ossifrage".

RSA-130

RSA-130 has 130 decimal digits (430 bits), and was factored on April 10, 1996 by a team led by Arjen K. Lenstra and composed of Jim Cowie, Marije Elkenbracht-Huizing, Wojtek Furmanski, Peter L. Montgomery, Damian Weber and Joerg Zayer.[10]

The value and factorization are as follows:

```
RSA-130 =
180708208868740480595165616440590556627810251676940134917012
70214

500566625402440483873411275908123033717818879665631820132140
880557

RSA-130 =
396859994595974542901611261628837860675764491128100648325555
157243
        ×
455344986467359721884036868972744088643563012632050696009990
044599
```

The factorization was found using the Number Field Sieve algorithm and the polynomial

$$574830224873840520 0\,x^5 + 98822619174822861 02\,x^4 - 133924993891281766 85\,x^3 + 168752524588776849 89\,x^2 + 37599001748552087 38\,x^1 - 467699305539319059 95$$

which has a root of 12574411168418005980468 modulo RSA-130.

RSA-140

RSA-140 has 140 decimal digits (463 bits), and was factored on February 2, 1999 by a team led by Herman te Riele and composed of Stefania Cavallar, Bruce Dodson, Arjen K. Lenstra, Paul Leyland, Walter Lioen, Peter L. Montgomery, Brian Murphy and Paul Zimmermann.[11][12]

The value and factorization are as follows:

```
RSA-140 =
212902463182587575474978820162715174978067039632772162782333
8321538194

998405649591136657385302191831678310738799531723088956923087
3441936471

RSA-140 =
339871742302843855453012362761387583563398649596959742349092
9302771479
        ×
626420018740128509615165494826444221930203717862350901911166
0653946049
```

The factorization was found using the Number Field Sieve algorithm and an estimated 2000 MIPS-years of computing time.

RSA-150

RSA-150 has 150 decimal digits (496 bits), and was withdrawn from the challenge by RSA Security. RSA-150 was eventually factored into two 75-digit primes by Aoki et al. in 2004 using the general number field sieve (GNFS), years after bigger RSA numbers that were still part of the challenge had been solved.

The value and factorization are as follows:

```
RSA-150 =
155089812478348440509606754370011861770654545830995430655466945774312632703

463465954363335027577729025391453996787414027003501631772186840890795964683

RSA-150 =
348009867102283695483970451047593424831012817350385456889559637548278410717
        ×
445647744903640741533241125787086176005442536297766153493419724532460296199
```

RSA-155

RSA-155 has 155 decimal digits (512 bits), and was factored on August 22, 1999 by a team led by Herman te Riele and composed of Stefania Cavallar, Bruce Dodson, Arjen K. Lenstra, Walter Lioen, Peter L. Montgomery, Brian Murphy, Karen Aardal, Jeff Gilchrist, Gerard Guillerm, Paul Leyland, Joel Marchand, François Morain, Alec Muffett, Craig Putnam, Chris Putnam and Paul Zimmermann.[13][14]

The value and factorization are as follows:

```
RSA-155 =
109417386415705274218097073220403576120037329454492059909138421314763499842889347847179972578912673324976257528997818337970765372440271467435315933544338 97

RSA-155 =
102639592829741105772054196573991675900716567808038066803341933521790711307779
        ×
106603488380168454820927220360012878679207958575989291522270608237193062808643
```

The factorization was found using the general number field sieve algorithm and an estimated 8000 MIPS-years of computing time.

RSA-160

RSA-160 has 160 decimal digits (530 bits), and was factored on April 1, 2003 by a team from the University of Bonn and the German Federal Office for Information Security (BSI). The team contained J. Franke, F. Bahr, T. Kleinjung, M. Lochter, and M. Böhm.[15][16]

The value and factorization are as follows:

```
RSA-160 =
215274110271888970189601520131282542925777358884567598017049767677813314521885913567301105977349105960249790711158521430207931466520284014061994699492757040775 3

RSA-160 =
454278928584813940716861906497388316561371457784697932509599847092500041573353594738809060383201619663383230378895197326892292104095794474135464881202849390936 7
```

The factorization was found using the general number field sieve algorithm.

RSA-170

RSA-170 has 170 decimal digits (563 bits), and was factored on December 29, 2009 by D. Bonenberger and M. Krone from Fachhochschule Braunschweig/Wolfenbüttel.[17]

The value and factorization are as follows:

```
RSA-170 =
260626236841398449215298792666744321970859253804864064161647851918599996285420693614502839319145146186835121981648059198820530572229741164780650958098323773365107115457595

RSA-170 =
358642073042850148679980458726852042329145968105997816114023186063394845085804059396 3
        ×
726702906410701907886379776392394626413613780385699667031370893600228158224958749449 3
```

The factorization was found using the general number field sieve algorithm.

RSA-576

RSA-576 has 174 decimal digits (576 bits), and was factored on December 3, 2003 by J. Franke and T. Kleinjung from the University of

Bonn.[18][19][20] A cash prize of US$10,000 was offered by RSA Security for a successful factorization.

The value and factorization are as follows:

```
RSA-576 =
188198812920607963838697239461650439807163563379417382700763356422988859715 23

4665485319

060606504743045317388011303396716199692321205734031879550656996221305168759 30

7650257059

RSA-576 =
398075086424064937397125500550386491199064362342526708406385189575946388957261768583317
        ×
472772146107435302536223071973048224632914695302097116459852171130520711256363590397527
```

The factorization was found using the general number field sieve algorithm.

RSA-180

RSA-180 has 180 decimal digits (596 bits), and was factored on May 8, 2010 by S. A. Danilov and I. A. Popovyan from Moscow State University, Russia.[21]

```
RSA-180 =
191147927718986609689229466631454649812986246276667354864188503638807260703 4

367990587762013651351612781342582961281092000467029129845687528003302217777 5

27739574045404957078514210 41

RSA-180 =
400780082329750877952581339104100572526829317815807176564882178998497572771950624613470377
        ×
476939688738611836995535477357070857939902076027788232031989775824606225595773435668861833
```

The factorization was found using the general number field sieve algorithm implementation running on 3 Intel Core i7 PCs.

RSA-190

RSA-190 has 190 decimal digits (629 bits), and was factored by I. A. Popovyan from Moscow State University, Russia and A. Timofeev from CWI, Netherlands.[22]

```
RSA-190 =
1907556405060696491061450432646028861081179759533184460647975622318915025587

184175754054976155121593293492260464152630093238509246603207417247261215808

581859859389469454904817217564014234813

RSA-190 =
3171195257690152709485171289740475929805147316029450327784761927832793642798125654241572430961 9
        ×
6015260020444561641587641685526676183243543359471811072599763828083615704046048162535561940489 9
```

RSA-640

RSA-640 has 640 bits (193 decimal digits). A cash prize of US$20,000 was offered by RSA Security for a successful factorization. On November 2, 2005, F. Bahr, M. Boehm, J. Franke and T. Kleinjung of the German Federal Office for Information Security announced that they had factorized the number using GNFS as follows:[23][24][25]

```
RSA-640 =
3107418240490043721350750035888567930037346022842727545720161948823206440518081504556346829671723286782437916272

838033415471073108501919548529007337724822783525742386454014691736602477652346609
RSA-640 =
1634733645809253848443133883865090859841783670033092312181110852389333100104508151212118167511579
        ×
1900871281664822113126851573935413975471896789968515493666638539088027103802104498957191261465571
```

The computation took 5 months on 80 2.2 GHz AMD Opteron CPUs.

The slightly larger RSA-200 was factored in May 2005 by the same team.

RSA-200

Wikinews has related news: ***Two hundred digit number factored***

RSA-200 has 200 decimal digits (663 bits), and factors into the two 100-digit primes given below.

On May 9, 2005, F. Bahr, M. Boehm, J. Franke, and T. Kleinjung announced[26][27] that they had factorized the number using GNFS as follows:

```
RSA-200 =
27997833911221327870829467638722601621070446786955428537560
00992932612840010

76093456710529553608560618223519109513657886371059544820065
76775098580557613

579098734950144178863178946295187237869221823983


RSA-200 =
35324619344027701212726049781984643686711974001976250236493
03468776121253679

42320005854795652808834 9
        ×
79258699544783330333470858414800596877379758573642199607343
30341455767872818

15213538140930474018546 7
```

The CPU time spent on finding these factors by a collection of parallel computers amounted – very approximately – to the equivalent of 75 years work for a single 2.2 GHz Opteron-based computer.[26] Note that while this approximation serves to suggest the scale of the effort, it leaves out many complicating factors; the announcement states it more precisely.

RSA-210

RSA-210 has 210 decimal digits (696 bits) and was factored in September 2013 by Ryan Propper:[28]

```
RSA-210 =
24524664490027821197651766357308801846702678767833275974341
44517150616008300

38587216952208399332071549103626827191679864079776723243005
60059203563124656

12184658179041001318592996199338170121493350348758705510 67
```

```
RSA-210 =
435958568325940791799951965387214406385470910265220196318705482144524085345 2

75999740244625255428455944579
        × (times)
562545761726884103756277007304447481743876944007510545104946851094548396577 4

79473472146228550799322939273
```

RSA-704

RSA-704 has 704 bits (212 decimal digits), and was factored by Shi Bai, Emmanuel Thomé and Paul Zimmermann.[29] The factorization was announced July 2, 2012.[30] A cash prize of US$30,000 was previously offered for a successful factorization.

```
RSA-704 =
740375634795617128280467960974295731425931888892312890849362326389727650 34

028266276891996419625117843995894330502127585370118968098286733173273108 93

090055250511687706329907239638078671008609696253793465056379635 9

RSA-704 =
909121352959781887844065830260043748589260831032835872042851216896041152 86

409333678249507883679567568061 41
        × (times)
814385925911004526572780912628442933587789900216762788320091417242932436 01

330041167020032408287779702524 99
```

RSA-220

RSA-220 has 220 decimal digits (729 bits), and has not been factored so far.

```
RSA-220 =
226013852620340578494165404861019751350803891571977671832119776810944564 1817

966676608593121306582577250631562886676970448070001811149711863002112487 9281
```

```
994874820660701310665866460833279828035603792053919801399 46
496955261
```

RSA-230

RSA-230 has 230 decimal digits (762 bits), and has not been factored so far.

```
RSA-230 =
179694915979410667329161284495732461563675618080126000708 88
91883553172646

034149093349337224786865075523085586419992922181443668472 28
74052065257937

495694348389263171152522525654410980819170611742509702440 71
80103648316382

88518852689
```

RSA-232

RSA-232 has 232 decimal digits (768 bits), and has not been factored so far.

```
RSA-232 =
100988139787192354690956489430946858281823382195557395514 11
20516205831021338

528545374366109757154363664913380084917065169921701524733 29
43892702802343809

609098049764405407112019654107475538249486727713740750115 77
18230539834060616

2079
```

RSA-768

RSA-768 has 232 decimal digits (768 bits), and was factored on December 12, 2009 by Thorsten Kleinjung, Kazumaro Aoki, Jens Franke, Arjen K. Lenstra, Emmanuel Thomé, Pierrick Gaudry, Alexander Kruppa, Peter Montgomery, Joppe W. Bos, Dag Arne Osvik, Herman te Riele, Andrey Timofeev, and Paul Zimmermann.[31]

```
RSA-768 =
123018668453011775513049495838496272077285356959533479219 73
224521517264005

072636575187452021997864693899564749427740638459251925573 26
303453731548268
```

```
507917026122142913461670429214311602221240479274737794080665
35141959745985

6902143413

RSA-768 =
33478071698956898786044169848212690817704794983713768568912
431388982883793

87800228761471165253174308773781446799948 9
        ×(times)
36746043666799590428244633799627952632279158164343087642676
032283815739666

51127923337341714339681027009279873630891 7
```

RSA-240

RSA-240 has 240 decimal digits (795 bits), and has not been factored so far.

```
RSA-240 =
12462036678171878406583504460810659043482037465167880575481
87888832896668011

88210855036039570272508747509864768438458621054865537970253
93057189121768431

82863628469484053016144164304680668756994152469931857041830
30512549594371372

159029236099
```

RSA-250

RSA-250 has 250 decimal digits (829 bits), and has not been factored so far.

```
RSA-250 =
21403246502407449612644230728393335630086147151447550177977
54920881418023447

14013664334551909580467961099285187247091458768739626192155
73630474547705208

05119056493106687691590019759405693457452230589325976697471
68173806936489469

9871578494975937497937
```

RSA-260

RSA-260 has 260 decimal digits (862 bits), and has not been factored so far.

```
RSA-260 =
22112825529529666435281085255026230927612089502470015394413
74831912882294140

20019865127297265697465990859003300314000511707422045608592
76357953757185954

29883895870922923849100670303412462054578456641366454068421
43612930176940208

463910658759147942514351444581 99
```

RSA-270

RSA-270 has 270 decimal digits (895 bits), and has not been factored so far.

```
RSA-270 =
23310853034440754452763765691068052414561981248030544904294
86119684959182451

35782867888369318577116418213919268572658314913060672626911
35402760979316634

16266939465961964277442738866018768963134687040590667469031
23910748277606548

64915192081269930976658751473545659 4993207
```

RSA-896

RSA-896 has 896 bits (270 decimal digits), and has not been factored so far. A cash prize of $75,000 was previously offered for a successful factorization.

```
RSA-896 =
41202343698665954385553136533257594817981169984432798284545
562643387644556

52484261980988704231618418792614202471888694925609317763750
334211309823974

85150944909106910269861031862704114880866970564902903653658
867433731720813

104105190864254793282601391257624033946373269391
```

RSA-280

RSA-280 has 280 decimal digits (928 bits), and has not been factored so far.

```
RSA-280 =
1790707753365795418841729699379193276395981524363782327873
18589639655966058

5783742549640396449103593468573113599487089842785784500698
716853446786525536

5503525160280656363736307175332772875499505341538927978510
751699922197178159

772473318427953447723956678917353236635727058310678 9
```

RSA-290

RSA-290 has 290 decimal digits (962 bits), and has not been factored so far.

```
RSA-290 =
3050235186294003157769199519894966400298217959748768348671
52661867331608769 4

3419156362946151249328917515864630224371171221716993844781
534383325603218163

2549201100649908073932858897185243836002511996505765970769
029474322210394327

6057515762835729207549593766420619956557868130913504412185
4119
```

RSA-300

RSA-300 has 300 decimal digits (995 bits), and has not been factored so far.

```
RSA-300 =
2769315567803442139028689061647233092237608363983953254005
03672280937582471 4

9473946190060218756255124317186573105075074546238828817121
274630072161346956

4396741836389979086904304472476001839015983033451909174663
464663867829125664

4598955751571788169002287927112674719583575744167143664997
220900156740 47
```

RSA-309

RSA-309 has 309 decimal digits (1,024 bits), and has not been factored so far.

```
RSA-309 =
133294399882575758380143779458803658621711224322668460285458826191727627667
0

542554046742693334919501552734933431407182284074635735280036866652127405759
1

187012833915749907235117966673965850342993102198516071411314672027736500662
3

692721807916355914275519065334791400296725853788916042959771420436564784273
9

10949
```

RSA-1024

RSA-1024 has 1,024 bits (309 decimal digits), and has not been factored so far. US$100,000 was previously offered for factorization.

Successful factorization of RSA-1024 has important security implications for many users of the RSA public-key authentication algorithm, as the most common key length currently[when?] in use is 1024 bits.

```
RSA-1024 =
135066410865995223349603216278805969938881475605667027524485143851526510
60

485953383394028715057190944179820728216447155137368041970396419174304649
65

892742562393410208643832021103729587257623585096431105640735015081875106
76

594629205563685529475213500852879416377328533906109750544334999811150056
97

7236890927563
```

RSA-310

RSA-310 has 310 decimal digits (1,028 bits), and has not been factored so far.

```
RSA-310 =
184821039782585067038014851770255937140089974525451252192570744558033471060
1

412527675708297932857843901388104766898429433126419139462696524583464983724
6

516314818884733641513687362363177835875184650170871454167340264246156906116
2

011638098248412085768848367657609486593018836714138879545437867134338625829
1

687641
```

RSA-320

RSA-320 has 320 decimal digits (1,061 bits), and has not been factored so far.

```
RSA-320 =
213681069641007179601208741450037729586376793837279335231506862036319655235
7

883709408543500095170094337383832199722056416630248832159012806153128501063
6

857163897899811712284013921068534616772684717323224436400485097837112174432
1

827034365483575406101750313713648930343799636722491521204470447299799616089

2591129924218437
```

RSA-330

RSA-330 has 330 decimal digits (1,094 bits), and has not been factored so far.

```
RSA-330 =
121870863310605869313817398014332524915771068622605522040866660001748138323
8

135245680242590355588072280526111107908988230371763263885614090933377863089

063482816790040500611272743217217997642701713779260695142499528183938370835
4

636468483926114931976844939654102090966520978986231260960498370992377930421
7
```

```
018624446552446986967592 67
```

RSA-340

RSA-340 has 340 decimal digits (1,128 bits), and has not been factored so far.

```
RSA-340 =
269098706229469511199648465800836187593130873035749649023967242993321569 4995

275858877122326330883664971511275673199794677960841323240693443353204889 8585

917667658075223156388439480762207617758662597397523612752281113660011041 5063

000469112815210681204287228569773514510502696683064954000365992261839969 4276

990464815739966698956947129133275233
```

RSA-350

RSA-350 has 350 decimal digits (1,161 bits), and has not been factored so far.

```
RSA-350 =
265071999517353947344981209737368110152978646421158316246745454822934458 5504

349584119150441334912456019316047814652843370780771686539198282306175141 9151

606849655575049676468644737917071142487312863146816801954812702917123189 2127

288682592826323938344439894820964980002198783774200949834726366790897650 1360

338232297255220406880606182953552982073164015 1
```

RSA-360

RSA-360 has 360 decimal digits (1,194 bits), and has not been factored so far.

```
RSA-360 =
218682020234317263146640637228579265464915856482838406521712186637422774 5448
```

```
776496388968081733421164363775215799496951698453948248667814130475167219752
4
```

```
005235057624723878512933800275740689262997074821273466378195217074591660916
8
```

```
935837235996278783280225742175701130252626518426356562342682345652253987471
7
```

```
615910191139267256230956065664579182406147670138065906491
```

RSA-370

RSA-370 has 370 decimal digits (1,227 bits), and has not been factored so far.

```
RSA-370 =
188828770723438397284270312799712727247091051938771806238098552300498707670
1
```

```
721281993726195254903980001896112258671262466144228850274568145436317048469
0
```

```
737944952503479749432169435214627132029657962372663109482249345567254149154
4
```

```
270099315287923527277926657829220716103274629754608002579386403054361786262
0
```

```
878802244305286292772467355603044265985905970622730682658082529621
```

RSA-380

RSA-380 has 380 decimal digits (1,261 bits), and has not been factored so far.

```
RSA-380 =
301350044312021160035658602410127699249216799779583920352836323661057856579
1
```

```
827075093740790189807021984362282109098064147705685005651479933662534967854
9
```

```
218794180711634478735831265177285887805862071748980072533360656419736316535
8
```

```
223777926342350195264684757967871182572073373273416986640614542528658166575
5
```

```
697726076355332825242157463301133511203173339339716835058551952447854174731
1
```

RSA-390

RSA-390 has 390 decimal digits (1,294 bits), and has not been factored so far.

```
RSA-390 =
268040194118238845450103707934665606536694174908285267872982242439770917825
0

462300247284896760428256233167631364541367246768499611881289973445122821298
9

163008475948506342360491163909958518683309401995768755037783497780340065362
8

695534490436743728187025341405841406315236881249848600505622302828534189804
0

079544743586503304624875147529741239869708808432103717639228831278554440220
9

1083492089
```

RSA-400

RSA-400 has 400 decimal digits (1,327 bits), and has not been factored so far.

```
RSA-400 =
201409687894520751172670048578344254791532178207270435610303912900996679339
6

141985086509455102260403208695558793091390340438867513766123418942845301603
2

619119305676856486261532125663001026834647174783659713139894314068546405163
1

751940314929430873730232168484095639518322211746844357850984794711999537364
5

360710979599471328761075043464682551112058642299370598078702810603300890715
8

74500584758146849481
```

RSA-410

RSA-410 has 410 decimal digits (1,360 bits), and has not been factored so far.

```
RSA-410 =
196536014799387614142394527417874570792626929443988074682797
1120992517421770

107913813932453903338107775554083034298964363339413753898335
5218902490897764

441296847433275460853182355059915490590169155909870689251647
7785203855688127

063506937209156459433352815650129392413318670514148513785684
574176615015943 7

606324416304008818088708702877171732193225299256775607526444
1680858665410918

43122321536802534985424358839
```

RSA-420

RSA-420 has 420 decimal digits (1,393 bits), and has not been factored so far.

```
RSA-420 =
209136630247651073165255642316333073700965362660524505479852
2959941292730258

189837357007618875260974964895352548492546639480050916921934
4906273145413634

242718626619709784602296924857945491615563368638810696236533
7549155747268356

466658384680996435419155013602317010591744105651749369012554
5320242581503730

340595288782692581391268394275643111482029231319370535271616
5790132673270514

381774416410760173541378588683657820797 9
```

RSA-430

RSA-430 has 430 decimal digits (1,427 bits), and has not been factored so far.

```
RSA-430 =
353463564562027136154120920960789722473488710618230709329200
5188843884213420
```

```
6950355315163258889704268733101305820000124678051064321160104990089741386777

2424190744453885127173046498565488221441242210687945185565975582458031351338

2070785777831859308900851761495284515874808406228585310317964648830289141496

3289966226854692560410075067278840383808716608668377947047236323168904650235

700922464739154420265499558659317095424686481095417
```

RSA-440

RSA-440 has 440 decimal digits (1,460 bits), and has not been factored so far.

```
RSA-440 =
2601428211955602590070788487371320550539810804595235289423508589669

3391270837431025267480059242674631900797889006533757316054194286819

1406564385332722948450299423322261711239266063575232577368936674527

3411922479051683878936845248180307729497304959710847337973805145677

3263119916483529703607405432752966630781223459776639075044144531447

0817180207090407273927593041029935900605961930559070193962772529617
          162999460598984421039594122215182134073704917
```

RSA-450

RSA-450 has 450 decimal digits (1,493 bits), and has not been factored so far.

```
RSA-450 =
1984634237142836623497230721861131427789462869258862089878538009871598692569

0078791591684242367262529704652673686711493985446003494265587358393155378115
```

```
80324470611551451607705809268243665732119939816626146357348
12647448360573856

31322474917155269972781155149056189532534439574358815035934
14842367096046182

76434347948498243152515106628556992696242074513657383842554
97823390996283918

32876674191729880722219965324033002589060832111607445081910
24837057033
```

RSA-460

RSA-460 has 460 decimal digits (1,526 bits), and has not been factored so far.

```
RSA-460 =
17868560204040044332621037892128445858864000869938829550810
51578507634807524

14640788198121696813944457714763346084886877462543182928286
03396149562623036

35645546753552581286559710032014178315212224644686666427660
44146641933788836

89324522173213548604843532961314038211758628909985986538583
73835628654351880

48063622316430823868487310523501157767155211494537088684281
08303016983133390

04163655154668570049008475016448080768256389182668489641536
26486460448430073

4909
```

RSA-1536

RSA-1536 has 463 decimal digits (1,536 bits), and has not been factored so far. $150,000 was previously offered for successful factorization.

```
RSA-1536 =
18476997032117414743068356202001644030185493386634101714717
857749106516967

11161249859337684305435744585616061544571794052229717732524
660960646946071
```

```
249623720442022269756756687378427562389508764678440933285157
49657884341508

847552829818672645133986336493190808467199043187438128336350
27954702826532

978029349161558118810498449083195450098483937752272570525780
591944993870073

695755688436933812779613089230392569695253261620823676490316
03655137144791

3932347169566988069
```

RSA-470

RSA-470 has 470 decimal digits (1,559 bits), and has not been factored so far.

```
RSA-470 =
170514737846811852090815992388870280251832558521491596835880
91836980967539803

689771144238360252631451919236661227059581551031197088611676
63177669964411814

095748660238871306469830461919135901638237924444074122866545
5229545368837485

587445521289504452180962081887888763243950493623768065799410
5330538621759598

404770960395431244769272527688759459065879293992460926126478
8857203221233 4726

855302571883565912645432522077138010357669555555071044090857
0895393205649635

76770285413369
```

RSA-480

RSA-480 has 480 decimal digits (1,593 bits), and has not been factored so far.

```
RSA-480 =
302657075295090869739730250315591803589112283576939858395529
6326343059761445

714416965981704012518521591385334559821723437123133832477321
0726853524776378
```

```
4105186549246199888070331088462855743520880671299302895546822695492968577380

706795842802200829411198422297326020823369315258921162990168697393348736236
0

812966041851456906399528297817679014976052139554853281419653467697425974793
0

685864584926832898568742388185363260470617556446171939611731829867982078549
1

87567494670041368093210 3
```

RSA-490

RSA-490 has 490 decimal digits (1,626 bits), and has not been factored so far.

```
RSA-490 =
186023912707684651719836935402607687526951593059283915020102835383703102597
1

373852216474332794920643399906822553185507255460678213880084116286603739332
4

657817180420171722244995403031529354787140136296150106500248655268866341574
5

975892579359416565102078922006731141692607694977776760490610706193787354060
1

594274731617619377537419071307115490065850326946551649682856865437718319058
6

953764069804493263889349245791475085585898084919048838531507692245375552748
1

137671909614411939005219902771569 1
```

RSA-500

RSA-500 has 500 decimal digits (1,659 bits) and has not been factored so far.

```
RSA-500 =
189719413374862665633053474331720252723718359195342830318458112306245045887
0

768760594321234762576642749455476441951542758674320565931725466994660498241
9
```

```
730160103812521528540068803151640161162396312837062979326593940508107758169
4
```

```
478604172141102464103804027870110980866421480002556045468762513774539341822
1
```

```
549482127733567173515347265632844800113494092644243844019891090860325267881
4
```

```
785060113207728717281994244511323201949222955423789860663107489107472242561
7
```

```
396803191692438146762357129342922999744113613
```

RSA-617

RSA-617 has 617 decimal digits (2,048 bits) and has not been factored so far.

```
RSA-617 =
227018012937850141935804051202045867410612359627665839070940218792151714831
1
```

```
913989487013309111104490168340094948384681829951804176350794892259077492546
6
```

```
088171879259465921026597046700449819899096862039460017743094473811056991294
1
```

```
285428918808553627074076707225937377726669734409773612433363973080517630915
0
```

```
683631079531260723952036529003210584883950798145230729941718571579629745499
5
```

```
023505316040919859193718023307414880446217922800831766040938656344571034778
5
```

```
534571210805307363945359239326518660305150410609664373133236728315393235000
6
```

```
793710754195543736243324836124252594586880235391676618153237585550488690143
2
```

```
221349733
```

RSA-2048

RSA-2048 has 617 decimal digits (2,048 bits). It is the largest of the RSA numbers and carried the largest cash prize for its factorization,

US$200,000. The largest factored RSA number is 768 bits long (232 decimal digits), and the RSA-2048 may not be factorizable for many years to come, unless considerable advances are made in integer factorization or computational power in the near future.

```
RSA-2048 =
25195908475657893494027183240048398571429282126204032027777
13783604366202070

75955562640185258807844069182906412495150821892985591491761
84502808489120072

84499268739280728777673597141834727026189637501497182469116
50776133798590957

00097330459748808428401797429100642458691817195118746121515
17265463228221686

99875491824224336372590851418654620435767984233871847744479
20739934236584823

82428119816381501067481045166037730605620161967625613384414
36038339044149526

34432190114657544454178424020924616515723350778707749817125
77246796292638635

63732899121548314381678998850404453640235273819513786365643
91212010397122822

120720357
```

See also

- Integer factorization records
- RSA Factoring Challenge (includes table with size and status of all numbers)
- RSA Secret-Key Challenge

Notes

1. **Jump up ^** RSA Laboratories, The RSA Factoring Challenge. Retrieved on 2008-03-10.
2. **Jump up ^** RSA Laboratories, The RSA Factoring Challenge FAQ. Retrieved on 2008-03-10.

3. **Jump up** ^ "RSA- 100 Factored". *Cryptography Watch Archive for April, 1991*. 1991-04-01. Retrieved 2008-08-05.

4. **Jump up** ^ "RSA Honor Roll". 1999-03-05. Retrieved 2008-08-05.

5. ^ Jump up to: *a* *b* Brandon Dixon and Arjen K. Lenstra. "Factoring Integers Using SIMD Sieves". doi:10.1007/3-540-48285-7.

6. **Jump up** ^ T. Denny, B. Dodson, A. K. Lenstra, M. S. Manasse (1994), "On The Factorization Of RSA-120" .

7. **Jump up** ^ "RSA Honor Roll". 1999-03-05. Retrieved 2008-08-06.

8. **Jump up** ^ "The Magic Words Are Squeamish Ossifrage". Retrieved 2009-11-24.

9. **Jump up** ^ Mark Janeba (1994), Factoring Challenge Conquered. Retrieved on 2008-03-10.

10. **Jump up** ^ Arjen K. Lenstra (1996-04-12), Factorization of RSA-130. Retrieved on 2008-03-10.

11. **Jump up** ^ Herman te Riele (1999-02-04), Factorization of RSA-140. Retrieved on 2008-03-10.

12. **Jump up** ^ RSA Laboratories, RSA-140 is factored!. Retrieved on 2008-03-10.

13. **Jump up** ^ Herman te Riele (1999-08-26), New factorization record (announcement of factorization of RSA-155). Retrieved on 2008-03-10.

14. **Jump up** ^ RSA Laboratories, RSA-155 is factored!. Retrieved on 2008-03-10.

15. **Jump up** ^ Jens Franke (2003-04-01), RSA-160 (announcement of factorization). Retrieved on 2008-03-10.

16. **Jump up** ^ RSA Laboratories, RSA-160 is factored!. Retrieved on 2008-03-10.

17. **Jump up ^** D. Bonenberger and M. Krone, RSA-170 Retrieved on 2010-03-08.

18. **Jump up ^** Jens Franke (2003-12-03), RSA576 (repost of announcement of the factorization). Retrieved on 2008-03-10.

19. **Jump up ^** Eric W. Weisstein (2005-12-05), RSA-576 Factored at MathWorld. Retrieved on 2008-03-10.

20. **Jump up ^** RSA Laboratories, RSA-576 is factored!. Retrieved on 2008-03-10.

21. **Jump up ^** S.A. Danilov and I.A. Popovyan *Factorization of RSA-180* PDF. Retrieved on 2010-05-12.

22. **Jump up ^** I. Popovyan, A. Timofeev (2010-11-08). "RSA-190 factored". *mersenneforum.org*. Retrieved 2010-11-10.

23. **Jump up ^** RSA Laboratories, RSA-640 is factored!. Retrieved on 2008-03-10.

24. **Jump up ^** Jens Franke (2005-11-04), We have factored RSA640 by GNFS. Retrieved on 2008-03-10.

25. **Jump up ^** Eric W. Weisstein (2005-11-08), RSA-640 Factored at MathWorld. Retrieved on 2008-03-10.

26. ^ Jump up to: *a* *b* Thorsten Kleinjung (2005-05-09), We have factored RSA200 by GNFS. Retrieved on 2008-03-10.

27. **Jump up ^** RSA Laboratories, RSA-200 is factored!. Retrieved on 2008-03-10.

28. **Jump up ^** RSA-210 factored, mersenneforum.org

29. **Jump up ^** Factorisation of RSA-704 with CADO-NFS.

30. **Jump up ^** Bai, Shi (2012-07-02). "Factorization of RSA704". *NMBRTHRY mailing list*. Retrieved 2012-07-03.

31. **Jump up ^** Cryptology ePrint Archive: Report 2010/006

References

- RSA Factoring Challenge Administrator (1997-10-12), RSA Challenge List.

- RSA Laboratories, The RSA Challenge Numbers (archived by the Internet Archive in 2006 before the RSA challenge ended).
- RSA Laboratories, Challenge numbers in text format.
- Kazumaro Aoki, Yuji Kida, Takeshi Shimoyama, Hiroki Ueda, GNFS Factoring Statistics of RSA-100, 110, ..., 150, Cryptology ePrint Archive, Report 2004/095, 2004.

External links

- RSA Laboratories, The RSA Factoring Challenge.
- Burt Kaliski (1991-03-18), RSA factoring challenge, the original challenge announcement on sci.crypt.
- Steven Levy (March 1996), Wisecrackers in Wired News. Has coverage on RSA-129.
- Weisstein, Eric W., "RSA Number", *MathWorld*.
- Eric W. Weisstein, Mathematica package for RSA numbers.

Categories:

- RSA Factoring Challenge
- Integer factorization algorithms
- Large integers
- This page was last modified on 4 February 2014 at 20:50.
-

END WIKIPEDIA “RSA numbers” posting

---

wikipedia "RSA Secret-Key Challenge" posting

(mouse copied exactly including misspelled words)

Hyperlinks have been preserved for posterity

RSA Secret-Key Challenge

From Wikipedia, the free encyclopedia

The **RSA Secret-Key Challenge** consisted of a series of cryptographic contests organised by RSA Laboratories with the intent of helping to demonstrate the relative security of different encryption algorithms. The challenge ran from 28 January 1997 until May 2007.[1]

Contents

Contest details

For each contest, RSA had posted on its website a block of ciphertext and the random initialization vector used for encryption. To win, a contestant would have had to break the code by finding the original plaintext and the cryptographic key that will generate the posted ciphertext from the plaintext. The challenge consisted of one DES contest and twelve contests based around the block cipher RC5.

Each of the RC5-* contests is named after the variant of the RC5 cipher used. The name *RC5-w/r/b* indicates that the cipher used *w*-bit words, *r* rounds, and a key made up of *b* bytes. The contests are often referred to by the names of the corresponding distributed.net projects, for example RC5-32/12/9 is often known as RC5-72 due to the 72-bit key size.

The first contest was **DES Challenge III** (and was also part of the DES Challenges), and was completed in just 22 hours 15 minutes by distributed.net and the EFF's Deep Crack machine.

In May 2007 RSA Laboratories announced the termination of the challenge, stating that they would not disclose the solutions to the remaining contents, and nor would they confirm or reward prize money for future solutions.[1] On 8 September 2008 distributed.net announced that they would fund a prize of $4000 for the RC5-72 contest.[2]

Distributed.net

The contests are associated with the distributed.net group, which had actively participated in the challenge by making use of distributed computing to perform a brute force attack.

RC5-32/12/7 was completed on 19 October 1997, with distributed.net finding the winning key in 250 days and winning the US$10,000 prize. The recovered plaintext was: *The unknown message is: It's time to move to a longer key length*.

RC5-32/12/8 also carried a US$10,000 prize and was completed by distributed.net on 14 July 2002. It took the group 1,757 days to locate the key, revealing the plaintext: *The unknown message is: Some things are better left unread*.

There were still eight remaining contests that had not yet been solved, **RC5/32/12/9** through to **RC5/32/12/16**, each of which was a US$10,000 prize. Distributed.net had been working on **RC5-32/12/9** and were over 1.950% through as of October 27, 2011.

See also

- RSA Factoring Challenge
- DES Challenges

External links

- Official contest page on the RSA website
- Current status of all contests within the challenge
- Unofficial status page on Distributed.net

- Distributed.net's RC5-72 Project Statistics

References

1. ^ Jump up to: [a] [b] Lawson, Jeff (2007-05-21). "bovine |21-May-2007 @ 04:34|". *blogs.distributed.net*. Retrieved 2010-08-01. "It is with great sadness that we must announce that RSA Labs has decided to terminate the RSA Secret-Key Challenge"

2. **Jump up ^** Lawson, Jeff (2008-09-08). "bovine |08-Sep-2008 @ 02:09|". *blogs.distributed.net*. Retrieved 2010-08-01. "Effective with this announcement, will officially fund the prize using the same distribution ratios that we would have originally used"

Categories:

- Cryptography contests
- Uncracked codes and ciphers
- 1997 establishments
- 2007 disestablishments
- This page was last modified on 14 March 2013 at 13:13.
- Text is available under the Creative Attribution-ShareAlike License

---

- **END WIKIPEDIA "RSA Secret-Key Challenge" posting**

The WOLFFRAM mathworld web site strictly prohibits copying so I will reference their page here but have also copied the current version for my own records of their sub-page entitled "RSA Number" in case they change their page. The link which has some out-dated and incomplete data is at the following link – (note there is no "www at the beginning so use the link exactly as written here) … mathworld.wolfram.com/RSANumber.html

---

The largest known prime numbers

The following is also mouse copied exactly as written in Wikipedia once again to preserve for posterity the misinformation that is being propagated by the controlled internet sources regarding prime numbers. As explained earlier in this book there is an entire fairy tale spun around the gee whiz announcements that a new and larger prime number has been found by supercomputers. The reality is that the searches are very narrow and based on the assumption that there is a higher probability of finding prime

numbers of the form $2^n - 1$ where n is very large also known as "Mersenne Primes". According to the latest findings at the time of this printing the number $2^{57,885,161} - 1$ is a prime number ever discovered with 17,425,170 digits. To many this may seem like a very large number. But compared to infinity it is a baby small insignificant eensy weensy number. The real issue however is that the tremendous amount of computing power it takes to achieve such a find may impress some, but the reality is that it does not provide even the least amount of understanding of prime numbers let alone predict where the next find might be found. Most of all it leaves enormous gaps in the finding of prime numbers that will never be filled in because the supercomputers and their handlers are already off looking for the next larger number to wow you, and the devil with all those other intermediate prime numbers.

The real understanding of what my Calculate Primes work has accomplished is that it not only gives order to the primes but provides theorems that show that the primes are an ever decreasing set with every application of The Generator Function which directly calculates the prime numbers in ever larger and larger groups with each succeeding application (see the book Calculate Primes for details). It further and most importantly allows one to calculate primes at any point along the number line (wherever you chose) without calculating all the prime numbers BUT if you so chose you can also directly calculate ALL of the prime numbers out to any designated size. Compare this to the brute force method that only produces by chance a few select numbers and gives no understanding of the order of the primes.

As a final point of reference, note that the largest known prime numbers using standard supercomputer techniques are much larger than the prime number factors of the RSA codes. The largest RSA "secure key" number is relatively small with only (for the largest to date) 617 digits and with its prime factors only having about half this number of digits.

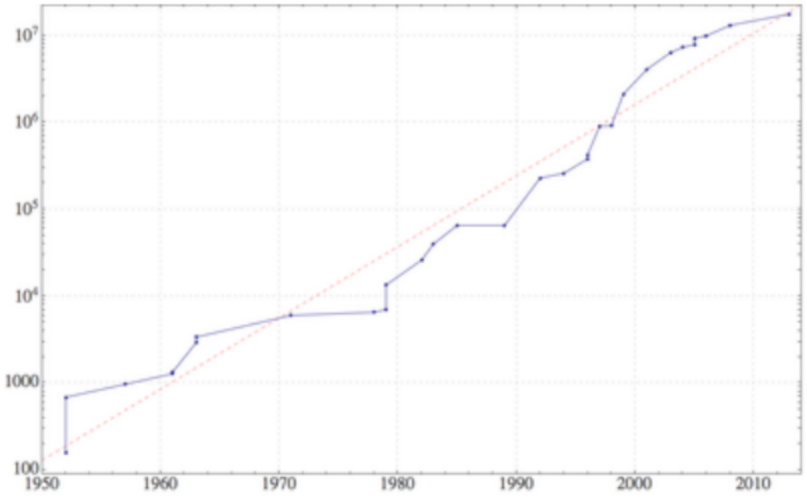
With this in mind read the "standard knowledge" Wikipedia posting regarding the largest known prime number. And feel free to not only calculate larger prime numbers in abundance using the Generator Function but also you will be able to calculate ALL the prime numbers out to these large numbers and far beyond with relative ease. Not only will you be able to go farther but you will also be able to relate all of your primes back to earlier generations of primes all the way back to the first prime building blocks 0 & 1 as detailed in the main text Calculate Primes.

Wikipedia "Largest known prime number"

Largest known prime number

From Wikipedia, the free encyclopedia

As of January 2014, the **largest known prime number** is $2^{57,885,161} - 1$,[1] a number with 17,425,170 digits.



Plot of the number of digits in largest known prime by year, since the electronic computer. Note that the vertical scale is logarithmic. The red line is the exponential curve of best fit: y = exp(0.188439 t - 362.591), where t is in years.

Euclid proved that there is no largest prime number. However, many mathematicians and hobbyists search for large prime numbers.

Many of the largest known primes are Mersenne primes. As of February 2013 the ten largest known primes are Mersenne primes, while the eleventh is the largest known non-Mersenne prime.[2] The last 15 record primes were Mersenne primes.[2]

The fast Fourier transform implementation of the Lucas–Lehmer primality test for Mersenne numbers is fast compared to other known primality tests for other kinds of numbers.

Contents

The current record

The record is currently held by $2^{57,885,161} - 1$ with 17,425,170 digits. Its discovery resulted from the Great Internet Mersenne Prime Search (GIMPS).

Prizes

There are several prizes offered by the Electronic Frontier Foundation for record primes.[3]

The record passed one million digits in 1999, earning a $50,000 prize.[4] In 2008 the record passed ten million digits, earning a $100,000 prize and a Cooperative Computing Award from the Electronic Frontier Foundation.[3] *Time* called it the 29th top invention of 2008.[5] Additional prizes are being offered for the first prime number found with at least one hundred million digits and the first with at least one billion digits.[3]

History

The following table lists the progression of the largest known prime number in ascending order. Here $M_n = 2^n - 1$ is the Mersenne number with exponent n.

Number	Digits	Year found
M_{127}	39	1876
$180 \times (M_{127})^2 + 1$	79	1951
M_{521}	157	1952
M_{607}	183	1952
M_{1279}	386	1952
M_{2203}	664	1952
M_{2281}	687	1952
M_{3217}	969	1957

M_{4423}	1,332	1961
M_{9689}	2,917	1963
M_{9941}	2,993	1963
M_{11213}	3,376	1963
M_{19937}	6,002	1971
M_{21701}	6,533	1978
M_{23209}	6,987	1979
M_{44497}	13,395	1979
M_{86243}	25,962	1982
M_{132049}	39,751	1983
M_{216091}	65,050	1985
$391581 \times 2^{216193} - 1$	65,087	1989
M_{756839}	227,832	1992
M_{859433}	258,716	1994
$M_{1257787}$	378,632	1996
$M_{1398269}$	420,921	1996
$M_{2976221}$	895,932	1997
$M_{3021377}$	909,526	1998
$M_{6972593}$	2,098,960	1999
$M_{13466917}$	4,053,946	2001
$M_{20996011}$	6,320,430	2003
$M_{24036583}$	7,235,733	2004
$M_{25964951}$	7,816,230	2005
$M_{30402457}$	9,152,052	2005
$M_{32582657}$	9,808,358	2006
$M_{43112609}$	12,978,189	2008
$M_{57885161}$	17,425,170	2013

The ten largest known prime numbers

Rank	Prime number	Found by	Found date	Number of digits	Reference
1st	$2^{57,885,161} - 1$	GIMPS	2013 January 25	17,425,170	[2]

2nd	$2^{43,112,609} - 1$	GIMPS	2008 August 23	12,978,189	[2]
3rd	$2^{42,643,801} - 1$	GIMPS	2009 April 12	12,837,064	[6]
4th	$2^{37,156,667} - 1$	GIMPS	2008 September 6	11,185,272	[6]
5th	$2^{32,582,657} - 1$	GIMPS	2006 September 4	9,808,358	[6]
6th	$2^{30,402,457} - 1$	GIMPS	2005 December 15	9,152,052	[7]
7th	$2^{25,964,951} - 1$	GIMPS	2005 February 18	7,816,230	[7]
8th	$2^{24,036,583} - 1$	GIMPS	2004 May 15	7,235,733	[7]
9th	$2^{20,996,011} - 1$	GIMPS	2003 November 17	6,320,430	[7]
10th	$2^{13,466,917} - 1$	GIMPS	2001 November 14	4,053,946	[7]

GIMPS found the 11 latest records on ordinary computers operated by participants around the world.

See also

- Mersenne prime
- Primality test
- Prime number

References

1. **Jump up ^** "GIMPS Project Discovers Largest Known Prime Number, $2^{57,885,161}$-1". *Mersenne Research, Inc.*
2. ^ Jump up to: *a b c d* Chris Caldwell, The largest known primes. Retrieved on 2013-02-05.
3. ^ Jump up to: *a b c* "Record 12-Million-Digit Prime Number Nets $100,000 Prize". *Electronic Frontier Foundation*. Electronic Frontier Foundation. October 14, 2009. Retrieved November 26, 2011.
4. **Jump up ^** Electronic Frontier Foundation, Big Prime Nets Big Prize.

5. **Jump up ^** "Best Inventions of 2008 - 29. The 46th Mersenne Prime". *Time*. Time Inc. Retrieved January 17, 2012.

6. ^ Jump up to: *a* *b* *c* Landon Curt Noll, Mersenne Prime Digits and Names. Retrieved on 2011-01-03.

7. ^ Jump up to: *a* *b* *c* *d* *e* Samuel Yates, Chris Caldwell, The largest known primes. Retrieved on 2014-03-08.

External links

- Press release about the largest known prime $2^{57,885,161}-1$
- Press release about the former largest known prime $2^{43,112,609}-1$
- Press release about an earlier largest known prime $2^{32,582,657}-1$

[hide]

- **v**
- **t**
- **e**

Prime number classes

By formula	• Fermat ($2^{2^n}+1$) • Mersenne (2^p-1) • Double Mersenne ($2^{2^{p-1}}-1$) • Wagstaff (2^p+1)/3 • Proth ($k\cdot 2^n+1$) • Factorial ($n!\pm 1$) • Primorial ($p_n\#\pm 1$) • Euclid ($p_n\#+1$) • Pythagorean ($4n+1$) • Pierpont ($2^u\cdot 3^v+1$)

	• Solinas ($2^a \pm 2^b \pm 1$) • Cullen ($n \cdot 2^n + 1$) • Woodall ($n \cdot 2^n - 1$) • Cuban ($x^3 - y^3)/(x - y$) • Carol $(2^n - 1)^2 - 2$ • Kynea $(2^n + 1)^2 - 2$ • Leyland ($x^y + y^x$) • Thabit ($3 \cdot 2^n - 1$) • Mills (floor(A^{3^n}))
By integer sequence	• Fibonacci • Lucas • Motzkin • Bell • Partitions • Pell • Perrin • Newman–Shanks–Williams
By property	• Lucky • Wall–Sun–Sun • Wilson • Wieferich • Wieferich pair • Fortunate • Ramanujan

	• Pillai • Regular • Strong • Stern • Supersingular (elliptic curve) • Supersingular (moonshine theory) • Wolstenholme • Good • Super • Higgs • Highly cototient • Illegal
Base-dependent	• Happy • Dihedral • Palindromic • Emirp • Repunit $(10^n - 1)/9$ • Permutable • Circular • Truncatable • Strobogrammatic • Minimal • Full reptend • Unique

	• Primeval • Self • Smarandache–Wellin
Patterns	• Twin (p, $p + 2$) • Bi-twin chain ($p - 1$, $p + 1$, $2p - 1$, $2p + 1$, …) • Triplet (p, $p + 2$ or $p + 4$, $p + 6$) • Quadruplet (p, $p + 2$, $p + 6$, $p + 8$) • Tuple • Cousin (p, $p + 4$) • Sexy (p, $p + 6$) • Chen • Sophie Germain (p, $2p + 1$) • Cunningham chain (p, $2p \pm 1$, …) • Safe (p, $(p - 1)/2$) • Arithmetic progression ($p + a \cdot n$, $n = 0, 1, \ldots$) • Balanced (consecutive $p - n$, p, $p + n$)
By size	• Titanic (1,000+ digits) • Gigantic (10,000+) • Mega (1,000,000+) • **Largest known**
Complex numbers	• Eisenstein prime • Gaussian prime
Composite numbers	• Pseudoprime • Almost prime

	• Semiprime • Interprime
Related topics	• Probable prime • Industrial-grade prime • Formula for primes • Prime gap

List of prime numbers

Categories:

- Prime numbers
- World records
- Superlatives
- This page was last modified on 17 March 2014 at 12:29.
- Text is available under the Creative Attribution-ShareAlike License

- **END WIKIPEDIA "Largest known prime number" posting**

THE END
