HyperSpace Security, Inc.’s Blog Post #1: Factoring

Welcome

Welcome to HyperSpace Security, Inc.’s blog!

HyperSpace offers a radical breakthrough in data security by eliminating the need to store a cryptographic master key, which is vulnerable to today’s computers and social engineering. With HyperSpace’s technology, master keys are never persistently stored and therefore cannot be hacked or stolen resulting in a “keyless” system. The technology not only protects against attacks based on quantum computing, it also provides unique benefits by securing payment systems, enhancing enterprise key management, bolstering multi-factor authentication, and securing blockchains and private key infrastructure.

In this forum, we will discuss issues related to data security, advances in mathematics and quantum computing, vulnerabilities of blockchains and other security technologies to attack, hacks that have harmed real people in the real world, and more. Some of these posts will get a little deep into some math. That said, we will try to make the content understandable to anyone interested in these fields.

Please feel free to provide comments and feedback. We value your input!

Today’s Topic

The topic of today’s blog post is factoring, which is critical to data security. Most online data security is based on the difficulty of solving the problem of factoring large numbers. As explained in more detail below, due to advancements in math and today’s computers, it is now easier and faster than ever before to factor large numbers. The result? Just follow the news to see what company has been hacked today and will again be hacked tomorrow absent HyperSpace’s future-proof technology.

Why Do We Care?

Most data security for nearly everything you do online is based on the difficulty of solving the problem of factoring large numbers. Examples include security for communicating with your bank and utility companies, online shopping such as Amazon and eBay, and almost everything else you do online. If someone can factor big numbers, that security goes away. The bad actor can pretend to be you: access your accounts, spend your money, steal your data, and do all kinds of bad things.

What is Factoring?

Factoring is figuring out what numbers multiplied together result in a known number. For example, the factors of the number 15 are 3 and 5.

Factoring numbers is easy if the numbers are small. Doing so is tough if the numbers are big. For example, factoring numbers of bit size 256, 512, or 1024 was thought to be basically impossible.

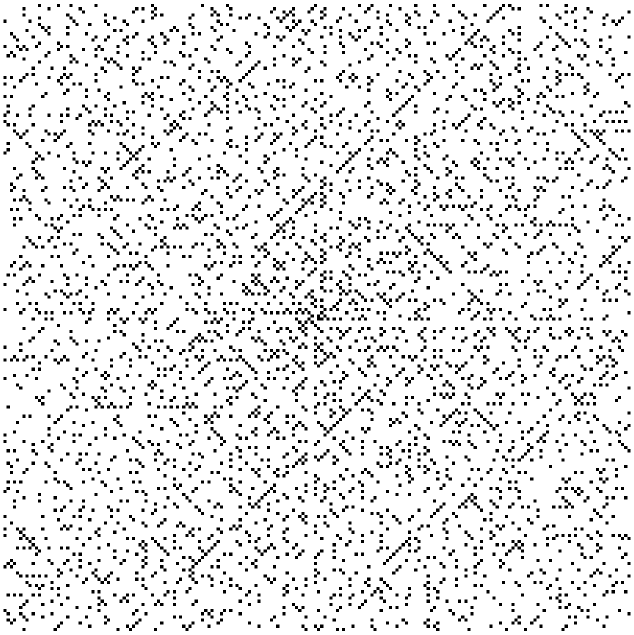
What do we mean by bit size? That's the number of ones and zeros needed to represent the number in a computer. An example of a 512-bit number in "hexadecimal" notation is 0x6CC061AD9DEF7C97C65C5E67FA74DDB303FED4DFCAB6FA2F6CC5414D7299A0DE4184F4B35A9E09A9AA400123F44DE2116C671D717A06816A9A0C6F9C2817BD71. Here, each digit represents 4 bits. Suffice to say this is a really big number.

Turns out advances have been made in mathematics that make factoring even these big numbers increasingly feasible. One example of such an advance is described here.

Some Math

Sorry, but now we have to get into some math to really explain what is going on here. If you are not into math, you can skip this part.

The new advancement we are discussing is based on the Ulam or prime number spiral. This spiral was devised by mathematician Stanislaw Ulam in 1963. The spiral is constructed by writing positive integers in a square spiral and specially marking the prime numbers. An image of a 200x200 Ulam Spiral follows:



See https://en.wikipedia.org/wiki/Ulam_spiral for a reasonably decent explanation.

How Does the Spiral Relate to Factoring?

We discovered the pattern of prime numbers shown in the Ulam spiral have applicability to the factoring problem: A number in the Ulam spiral close to another number often is a factor of or shares a common factor with that number. Determining numbers close to a number in the Ulam Sprial is easy.

Finding two numbers that share a common factor permits factorization of both numbers by determining their greatest common devisor using Euclid's algorithm. *See, e.g.,* https://en.wikipedia.org/wiki/Greatest_common_divisor.

Examples

A simple example is the number 15. The numbers adjacent to 15 in the Ulam spiral are 5, 16, 35, 4, 34, 3, 14, and 33. 5 and 3 are factors of 15. 35 and 33 share factors with 15.

Another example is the number 2183 with prime factors 37 and 59. The numbers adjacent to 2183 in the Ulam spiral are 2373, 2182, 1999, 2374, 2000, 2375, and 2001. None of these has a common factor with 2183. The numbers two away from 2183 in the Ulam Spiral include 2571, 2372, 2181, 1998, 1823, 2572, 1824, 2574, 1826, 1575, 2376, 2185, 2002, and 1827. 1998 has a common factor with 2183 of 37.

Extensions

Some extensions of the foregoing concepts have also been explored. One extension involves testing the numbers close to the number to be factored in the Ulam spiral squared +/-1 for a common factor. This extension found numbers with common factors more closely than under the base approach.

A further extension involves testing the close numbers cubed +/-1 for a common factor with the number at issue. This further extension also yielded significant results.

The Ulam Spiral itself can also be modified in the following manners: Instead of adding 1 to each step of the spiral, an even number that preferably is a multiple of 6 can be added. Also, the spiral can be started at an arbitrary odd number. For example, the core of a modified Ulam spiral could be the following:

1073742063	1073742051	1073742039	1073742027	1073742015
1073742075	1073741895	1073741883	1073741871	1073742003
1073742087	1073741907	**1073741823**	1073741859	1073741991
1073742099	1073741919	1073741835	1073741847	1073741979
1073742111	1073741931	1073741943	1073741955	1073741967

The highlighted starting point of this modified Ulam spiral is (2^30)-1, and each step of the spiral is +12.

Is this Real?

Yes.

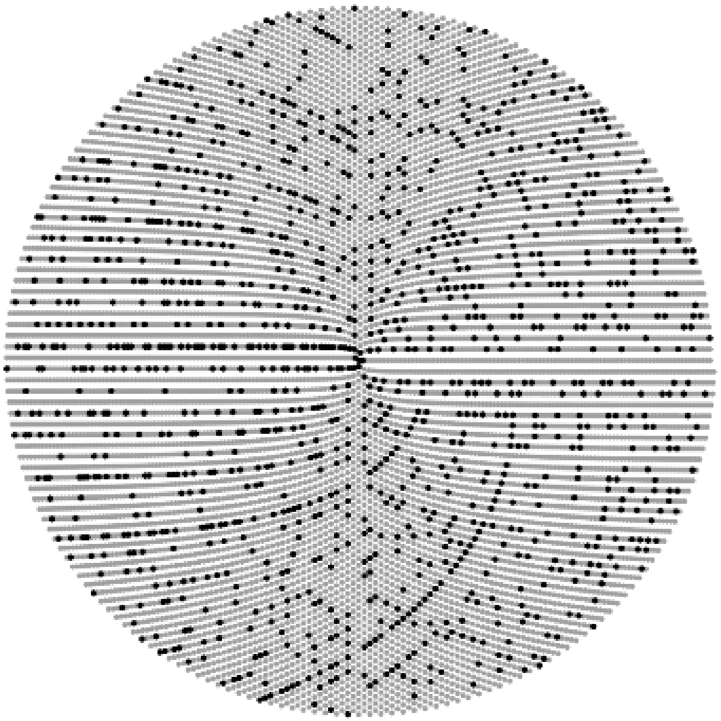
The base approach was used to factor every non-prime number less than or equal to 13,924 (slightly over 13 bits) with a simple Excel spreadsheet. The spreadsheet factored all of these numbers in a few seconds.

An Excel spreadsheet implementing one of the extensions successfully factored each and every one of over 13,000 30-bit numbers in a few seconds. You read that right: over 13,000 30-bit numbers were factored in a few seconds using a simple Excel spreadsheet!

Unfortunately, Excel cannot handle much larger numbers, so testing stopped at that point. Further testing is in the works using more sophisticated tools.

Areas for Further Study

Application of the foregoing techniques to related spirals especially Sacks Spiral



and Fermat's Spiral https://en.wikipedia.org/wiki/Fermat%27s_spiral may yield additional results of interest.

Another area for future study is extension of the spirals to higher dimensions. Progress has been made on this front.

Other Approaches

We are not the only people working on the problem of factoring large numbers. Many other approaches show promise. Some of the approaches are stronger for some types of numbers, and others are stronger for different types of numbers. A few very enterprising people have combined multiple approaches with great success.

Are We Using Some Special Type of Computer?

No. The testing was run on a simple off-the-shelf laptop computer.

What's Next?

Even more sophisticated approaches to the factoring problem using quantum computing exist. The next blog posts will address the reality of quantum computing, its breathtakingly rapid evolution, and its applicability to this and other problems including polynomial based secret sharing.

About the Author

Dane C. Butzer is the inventor of HyperSpace Security, Inc.'s Key Shadowing technology. He holds a Bachelor of Science in Electrical Engineering, a Master of Science, and a Juris Doctor, all from the Ohio State University. Mr. Butzer also has been published in Applied Optics and in the Appendix of the first edition of Bruce Schneier's seminal work *Applied Cryptography*. He has held several patents including currently issued U.S. Patent No. 9,634,836 for "Key Shadowing."

Peer review: This work has been peer reviewed by James DeCesare, a former Principal Architect at AT&T, and AJ Galiano, co-founder of SecureWorks, Inc. and BlueBox Studios, Inc.

For More Information

Questions can be posted on this blog. We will try to answer those questions. You can also follow us on Twitter @keyshadowing. Excel spreadsheets implementing the approaches discussed above will be provided to any interested party upon request to the author at dbutzer@keyshadowing.com.