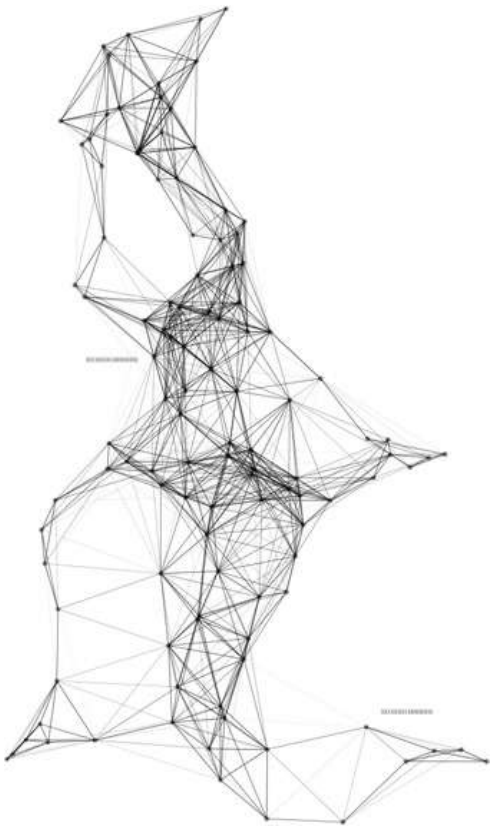
Check our Numbers

(tel:1.801.701.9600)
1.801.701.9600

The Math Behind Estimations to Break a 2048-bit Certificate

The Math: So you're interested in the math/science behind our claims in the SSL cracking video



(https://www.digicert.com/TimeTravel/)...? This is the basis of our assumptions...

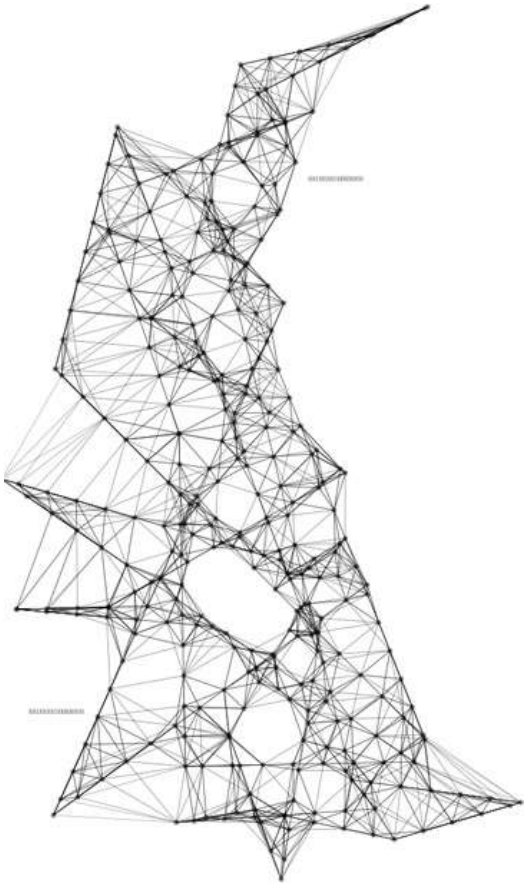
In order to "break" an RSA key based certificate like those provided by DigiCert, one must factor very large numbers that make up the RSA modulus. A certificate is considered "cracked" when the computer utilized reaches the average probability of time to factor the RSA modulus associated with the key in the certificate (in other words, it could happen in year 1 or it could happen in year 6 quadrillion, and the average would be half the time it eventually takes to efficiently try all possibilities). In December 2009, Lenstra et al announced the factorization of a 768-bit RSA modulus (see: http://eprint.iacr.org/2010/006.pdf) - this is a 232-digit number, and was at the time (and potentially still is) the record for factoring the largest general integer.

The most efficient method known to factor large integers, and the method used in the factorization record listed above, is via the number field sieve (NFS) - which is much faster than a brute force attack (where every combination is tried), so a brute force attack would have taken much longer than even this. The Lenstra group estimated that factoring a 1024-bit RSA modulus would be about 1,000 times harder than their record effort with the 768-bit modulus, or in other words, on the same hardware, with the same conditions, it would take about 1,000 times as long. They also estimated that their record achievement would have taken 1,500 years if they normalized processing power to that of the standard desktop machine at the time - this assumption is based on a 2.2 Ghz AMD Opteron processor with 2GB RAM.

So in other words, Lenstra et al claimed that it would take 1.5 million years with the standard desktop machine at the time, to repeat their record effort.

DigiCert's base standard is to use 2048-bit keys in secure SSL certificates - that is enormously stronger than anything Lenstra et al attempted, in fact, it would require factoring a 617-digit number. RSA Labs claim (see: http://www.rsa.com/rsalabs/node.asp?id=2004) that 2048-bit keys are 2^32 (2 to the power of 32) times harder to break using NFS, than 1024-

bit keys. 2^32 = 4,294,967,296 or almost 4.3 billion, therefore breaking a DigiCert 2048-bit SSL certificate (https://www.digicert.com/ssl-certificate/) would take about 4.3 billion times longer (using the same standard desktop processing) than doing it for a 1024-bit key. It is therefore estimated, that standard desktop computing power would take 4,294,967,296 x 1.5 million years to break a DigiCert 2048-bit SSL certificate. Or, in other words, a little over 6.4 quadrillion years.



In putting together our video, we estimated the age of the Universe to be 13,751,783,021 years or a little over 13.75 billion years*, therefore if you tried to break a DigiCert 2048-bit SSL certificate using a standard modern desktop computer, and you started at the beginning of time, you would have expended 13 billion years of processing by the time you got back to today, and you would still have to repeat that entire process 468,481 times one after the other into our far far distant future before there was a good probability of breaking the certificate. In fact the Universe itself would grow dark before you even got close.

The Art: A few concessions were made in the creation and visualization of these materials. The Big Bang shown is simply an artistic interpretation of the event. Most experts agree that there was no giant "explosion" at the start of time. Rather, the big bang is simply the expansion of the universe from an infinitely small source. Since space and time didn't exist before the Big Bang there would be no possible way to witness the start of the universe from outside the singularity. This is also assuming that there was a Big Bang as other models of the universe are equally valid if not as popular. Other astronomical events shown are also, obviously, artistic interpretations. Furthermore, the exact year each event took place is only as accurate as the generally accepted timeline of the universe. Taking into account the liberty the margin of error within that model will allow.

For more information see:

Big Bang Age: Komatsu, E.; Dunkley, J.; Nolta, M. R.; Bennett, C. L.; Gold, B.; Hinshaw, G.; Jarosik, N.; Larson, D. et al. (2009). "Five-Year Wilkinson Microwave Anisotropy Probe Observations: Cosmological Interpretation". Astrophysical Journal Supplement 180 (2): 330

First Stars: Ferreting Out The First Stars; http://www.physorg.com/news6689.html

Formation of Galaxies: "New Scientist" 14th July 2007

Age of our Solar System: A. Bouvier and M. Wadhwa. "The age of the solar system redefined by the oldest Pb-Pb age of a meteoritic inclusion."Nature Geoscience, in press, 2010. Doi: 10.1038/NGEO941

Age of the Earth: Dalrymple, G. Brent (2001). "The age of the Earth in the twentieth century: a problem (mostly) solved". Geological Society, London, Special Publications 190 (1): 205–221

Multi-cellular life (Proterozoic life): El Albani, Abderrazak; Bengtson, Stefan; Canfield, Donald E.; Bekker, Andrey; Macchiarelli, Reberto (July 2010). "Large colonial organisms with coordinated growth in oxygenated environments 2.1 Gyr ago". Nature 466 (7302): 100–104

Fate of the Sun: Schröder, K.-P.; Smith, R.C. (2008). "Distant future of the Sun and Earth revisited". Monthly Notices of the Royal Astronomical Society 386 (1): 155

End of the universe: A dying universe: the long-term fate and evolution of astrophysical objects, Fred C. Adams and Gregory Laughlin, Reviews of Modern Physics 69, #2 (April 1997), pp. 337–372