More About
Bulletins
Challenges
Crypto FAQ
CryptoBytes
RSA Algorithm
PKCS
Advanced Encryption Standard
Tech Notes
Staff & Associates
Standards

Has the RSA algorithm been compromised as a result of Bernstein's Paper?

April 8, 2002

Some recent articles have suggested that 1024-bit RSA keys are no longer secure. What's going on?

In a recent research paper [1], Daniel Bernstein, a mathematics professor at University of Illinois, observed that the cost of breaking an RSA key - the product of the amount of hardware needed and the running time - might not be as great for very large key sizes as previously thought.

Although Bernstein did not himself draw any conclusions about the security of practical RSA key sizes, such as 1024 bits (and has been careful to discourage early conclusions), newsgroup messages led to several articles speculating that 1024-bit RSA keys might be at risk [2][3][5][6][9].

Are 1024-bit RSA keys at risk?

They're no more at risk now than before Bernstein's paper appeared.

First, while Bernstein's paper suggests some very clever methods for reducing the amount of memory required to break very large RSA keys, his methods are all implementation techniques for the Number Field Sieve, currently the best method for factoring large numbers. The basic number of operations required by the Number Field Sieve, however, is not reduced. Since previous security estimates for 1024-bit RSA keys are based on the number of operations required by the Number Field Sieve, they still apply.

Second, while the methods introduced in the paper may reduce the cost of breaking very large RSA keys (the amount of hardware times the running time), RSA Laboratories finds that practical key sizes such as 1024 bits are not impacted by the new methods.

Finally, the recent concern [2] [3] [9] about the security of 1024-bit RSA keys is based in part on a misreading of Bernstein's paper. These references quote an estimate that for about $1 billion, a national agency could build a factoring machine based on Bernstein's design that could break a 1024-bit RSA key in a matter of "seconds to minutes". However, a factor of 10 billion or more was inadvertently left out of the running time in the preliminary analysis --- which means that the actual running time, assuming the machine could be built, would be measured in decades (see Note 1). Moreover, Bernstein himself is quoted [5] as saying "This is a theoretical advance. I have no idea and …nobody else has any idea how practical it might be."

The security of 1024-bit RSA keys is clearly not in jeopardy as a result of Bernstein's paper.

How hard is it to break a 1024-bit RSA key?

Arjen Lenstra and Eric Verheul [4] posit that by the year 2009, a machine that could break a 1024-bit RSA key in about a day would cost at least $250 million. This assumes that processor performance continues to double every 18 months,

following Moore's Law, and that factoring algorithms improve as well. Such a machine would probably cost about $160 billion today, which is consistent with a roughly 80-bit symmetric key size equivalent. (Note 2)

Robert Silverman gives a much higher estimate than Lenstra and Verheul, considering the amount of memory required by current implementations of the Number Field Sieve [8]. He estimates that a $10 million machine, using 2000 computer technology, would take about 3,000,000 years to break a 1024-bit RSA key. This gives a cost-based equivalent of about a 96-bit symmetric key, providing an additional margin of security. Not all researchers accept that memory cost will be an issue, however, and this margin will likely diminish over time as memory costs decrease.

RSA Security continues to actively promote and support these discussions on the cryptanalysis of the RSA algorithm. It is only through peer review that we can continue to ensure the strength of the RSA algorithm. The research of Bernstein and others is tremendously important to the field of cryptography and should be encouraged.

What key size should I be using?

NIST offered a table of proposed key sizes for discussion at its key management workshop in November 2001 [7]. For data that needs to be protected no later than the year 2015, the table indicates that the RSA key size should be at least 1024 bits. For data that needs to be protected longer, the key size should be at least 2048 bits.

RSA Laboratories considers these to be reasonable general guidelines, although the sensitivity of the data protected by the key must also be taken into account. In particular, root keys and other high-value organization keys should be at least 2048 bits, and users who are particularly cautious may wish to employ keys larger than 1024 bits sooner.

Do I need to revoke my 1024-bit RSA key?

The recent paper by Bernstein and the ensuing discussions don't reveal any new threats to 1024-bit RSA keys. You may, of course, decide that the security provided by a 1024-bit RSA key is less than you want for your (presumably long-term) application, and upgrade to a longer key. But you needn't do so just because of the recent discussion .

Notes

1. An informal panel was convened at the Financial Cryptography conference in March 2002 to discuss Bernstein's paper. At the panel, Nicko van Someren gave a rough estimate of the actual cost of breaking a 1024-bit RSA key using the ideas in Bernstein's paper. He suggested that the machine could be built for $1 billion and break a key in "seconds to minutes". These figures were quoted in a BugTraq posting [3] but the "seconds to minutes" figure was based on a small misreading of Bernstein's paper. RSA Laboratories' calculations indicate that the estimate omitted a factor of at least 10 billion, which suggests that without any other optimizations, and assuming the design is otherwise correct, the running time should be measured in decades. Assuming other optimizations, van Someren has subsequently stated that the machine would take "weeks". For a precise estimate, further research as well as implementation experience is needed.

2. Lenstra and Verheul's Table 1 indicates that with 2002 technology, a 768-bit RSA key is comparable to a 72-bit symmetric key in terms machine cost (see also Sec. 4.5 of [4]). The estimated cost with 2002 technology is about $160 million. A 1024-bit RSA key involves about 1000 times as many operations as a 768-bit RSA key with current methods, so is comparable to an 82-bit symmetric key in terms of machine cost (or even higher, if the additional memory cost is considered per [8]).

References

[1] D.J. Bernstein. *Circuits for Integer Factorization: A Proposal*. Manuscript, November 2001. http://cr.yp.to/papers.html#nfscircuit.

[2] Dennis Fisher. Experts debate risks to crypto. *e-Week*, March 27, 2002. http://www.eweek.com/article/0,3658,s=712&a=24663,00.asp.

[3] News Group Discussion. *1024-bit RSA Keys in Danger of Compromise*. BugTraq archive, March 24, 2002. http://online.securityfocus.com/archive/1/263924.

[4] Arjen K. Lenstra and Eric R. Verheul. Selecting cryptographic key sizes. *Journal of Cryptology*, to appear. http://www.cryptosavvy.com/.

[5] Vin McLellan. Factoring friction. *Information Security*, April 2002. http://www.infosecuritymag.com/2002/apr/news.shtml#factoringfriction.

[6] James Middleton. 1024-bit encryption is 'compromised'. *Vnunet.com*, March, 26, 2002. http://www.vnunet.com/News/1130451.

[7] NIST. *Key Management Guideline - Workshop Document*. Draft, October 2001. http://csrc.nist.gov/encryption/kms/key-management-guideline-(workshop).pdf.

[8] Robert D. Silverman. *A Cost-Based Security Analysis of Symmetric and Asymmetric Key Lengths*. RSA Laboratories Bulletin #13, April 2000. http://www.rsasecurity.com/rsalabs/bulletins/.

[9] Kevin Townsend. Bernstein's bombshell. *Internet World*, March 2002. http://www.internetworld.co.uk/IW/vRoot/articles/article.cfm?objectid=8A55E682-CDD4-4CB0-903C6093FE34E390.