More on RSA

There is more to RSA than the algorithm. How secure is it? I am using three sources here. The first is Schneier’s book, *Applied Cryptography*, which I’ve referred to before. Another is Steven Levy’s *crypto*, which is generally technically accurate and is written in a gonzo Tom Wolfe – Hunter S. Thompson style, which sometimes interferes with the accuracy; it’s kind of *The Right Stuff* meets *The Soul of a New Machine*. The last is Singh’s *The Code Book*.

The first public announcement of RSA was in Martin Gardiner’s column in *Scientific American*. The column was titled “A New Kind of Cipher That Would Take Millions if Years To Break,” and included a 129 digit public key and the promise of a $100 reward to anyone who could break it.

Gardiner was more of a magician than a mathematician, but was influential in some circles, if only because of the size and quality of his audience. When Persi Diaconis, a street magician, decided that he needed to get a PhD in Mathematics, he got a letter from Martin Gardiner, who noted that Diaconis’s proficiency in inventing card tricks (Diaconis’s card tricks are especially fascinating).

The time to crack was a rough estimate of the time it would take to factor the key based on known algorithms. But factoring is of interest in other areas, and it was inevitable that research on factoring would continue.

By current standards, 129 digits is not very much, and it only took four months for a distributed attack – that is, one implemented in parallel on many computers over the internet, an early version of SETI At Home – deciphered the message “the magic words are aquammous ossifrage.” [This attack, led by Arjen Lenstra, whose field is computational number theory, was launched 15 years after the article was published.]

The real point of all of this is that RSA has been subject to intense public and academic scrutiny for almost 30 years. Someone who breaks RSA has more to gain by making a public announcement than by keeping it a secret (assuming a rational, non-criminal cracker).

Implementation Issues

RSA has been implemented in software and hardware. It is 1000 times slower than DES in hardware, and 100 times slower than DES in software.

RSA is still very active in promoting security research and techniques; see

http://www.rsaconference.com/2007/us/content/webcasts/
Notice the list of speakers at this year’s RSA Conference: Bill Gates, Larry Ellison, Whitfield Diffie; let’s listen.