RSA, Factoring, and Squeamish Ossifrage

D. R. Stinson

The decryption in 1994 of the so-called "RSA challenge" ciphertext generated a considerable amount of publicity, and again brought the factoring problem to wide public attention. The computation was performed by Atkins, Graff, Lenstra and Leyland [1], with the help of about 600 other people. But let's first back up a bit and say something about the history of this problem.

The RSA cryptosystem was invented by R. Rivest, A. Shamir and L. Adleman in 1977. A research report [5] having the title "On Digital Signatures and Public-Key Cryptosystems" contained the first published description of the system. Then, in the February 1978 issue of the *Communications of the ACM*, the three authors published the paper [4] entitled "A Method for Obtaining Digital Signatures and Public-Key Cryptosystems". However, in the meantime, Martin Gardner devoted his "Mathematical Games" column in the August, 1977, issue of *Scientific American* to a discussion of the RSA cryptosystem [2]. This, of course, created an enormous amount of publicity for the RSA cryptosystem and for the idea of public-key cryptography in general.

It is interesting to read Martin Gardner's column today. He begins the column with the prediction that electronic mail will eventually replace traditional "paper" mail. He said:

> The transfer of information will probably be much faster and cheaper by "electronic mail" than by conventional postal systems.

Of course this is certainly the case today in the 1990's. However, I wonder how many people would have made such a prediction in 1977, when almost all computing was done by isolated mainframe computers and widespread use of personal computers was still a few years in the future.

Martin Gardner's next sentence is also very interesting, but for a different reason:

> Before long, it should be possible to go to any telephone, insert a message into an attachment and dial a number. The telephone at the other end will print out the message at once.

This prediction has also come true, but its realization is today called a "fax machine" as opposed to "e-mail" which is transmitted between computers.

Martin Gardner then goes on to describe the shift cipher and the one-time pad, before turning to RSA, which he called the "MIT Cipher" in his column. One of the fun things in his article is a sample of ciphertext whose decryption was posed as a challenge — this is the "RSA challenge" mentioned above.

Recall that the setting for the RSA cryptosystem is $\mathbb{Z}_n$, where $n = pq$, and p and q are distinct odd primes. In this situation, $\phi(n) = (p-1)(q-1)$. The encryption exponent b is chosen such that $\gcd(b, \phi(n)) = 1$, and the decryption exponent is defined to be

$$a = b^{-1} \bmod \phi(n).$$

Then the encryption function is $e_K(x) = x^b \bmod n$ and the decryption function is $d_K(y) = y^a \bmod n$.

In the RSA challenge, n is a 129-digit number, and the two prime factors have 64 and 65 digits. The public encryption exponent is $b = 9007$. In the *Scientific American* column, a prize of \$100 was offered to the first person to decrypt the message. (Actually, in a letter from R. Rivest to M. Gardner in April, 1977, an expiration date of April 1, 1982 for collecting the prize was given. However, no deadline was given in the "Mathematical Games" column, and the prize was eventually paid out, even though the expiration date had passed.)

In 1977, Rivest estimated that factoring a 129-digit number, using the best factoring algorithm at the time, would take 4×10^{13} years, even if modular multiplication could be done in 1 nanosecond. Modular multiplications still cannot be done this fast today, but nevertheless the modulus was factored in 1994, which is somewhat less than 40 quadrillion years. Of course what happened in the interim was that many new and more efficient factoring algorithms were developed.

For a nice recent article on the development of factoring algorithms in recent years — and for some predictions for the future — see Odlyzko [3]. Here we will summarize some of the progress in factoring in terms of "records in integer factorization". (Note that these "records" generally refer to numbers that are the product of two primes, and not of some "special form". It is of course not too difficult to factor special numbers of arbitrary length, for example, a 1 followed by one million zeroes!)

Odlyzko reports that numbers of 20 digits could be factored in 1964; numbers of 45 digits could be factored in 1974; numbers of 71 digits could be factored in 1984; and the RSA challenge broken in 1994 necessitated the factoring of a 129-digit number. This progress is due to a combination of faster computers and better algorithms. However, it is interesting to note that the algorithm used to factor the modulus in the RSA challenge is the Quadratic Sieve algorithm, which has been around since the early 1980's. The algorithm which is the object of the most current interest is the Number Field Sieve; this algorithm almost certainly will be faster for factoring larger numbers.

Even though the RSA challenge involved a 129-digit modulus, it was already recommended in 1978 by Rivest, Shamir and Adleman that n should preferably be a 200-digit modulus (the product of two 100-digit primes). Such a modulus would still be secure today.

Details of the factoring of the RSA challenge modulus can be found in [1]. The computation used about 1600 computers and required (very roughly!) about 4000-6000 MIPS-years of computation. The task was begun in August 1993 and completed on April 2, 1994. Of course, once the modulus was factored, it was a simple matter to compute $\phi(n)$, then to compute the decryption exponent a, and finally to decrypt the ciphertext. But, all in all, this does not seem to be a very cost-effective way of collecting a $100 prize!

By the way, the decrypted ciphertext is (of course!) as follows:

The magic words are squeamish ossifrage

References

[1] D. Atkins, M. Graff, A. K. Lenstra and P. C. Leyland. The Magic Words are Squeamish Ossifrage, in "Advances in Cryptology – ASIACRYPT '94", J. Pieprzyk and R. Safavi-Naini, eds., *Lecture Notes in Computer Science* **917**, (1995), 263–277. [Also available on the WWW: `http://draco.centerline.com:8080/~franl/crypto/`]

[2] M. Gardner. A New Kind of Cipher That Would Take Millions of Years to Break, *Scientific American*, August 1977, 120–124.

[3] A. Odlyzko. The Future of Integer Factorization, *CryptoBytes*, Summer 1995, 5–12. [Also available on the WWW: `ftp://netlib.att.com/netlib/att/math/odlyzko/index.html.Z`]

[4] R. Rivest, A. Shamir and L. Adleman. A Method for Obtaining Digital Signatures and Public-Key Cryptosystems, *Communications of the ACM* **21** (1978), 120–126.

[5] R. Rivest, A. Shamir and L. Adleman. On Digital Signatures and Public-Key Cryptosystems, *Technical Memo 82*, Laboratory for Computer Science, Massachusetts Institute of Technology, April, 1977.