Dr. Ron Rivest on the Difficulty of Factoring

(Since the difficulty of "cracking" the RSA algorithm has long been believed to be roughly equivalent to the difficulty of factoring a given RSA modulus, we have decided to reprint one of Ron Rivest's classic papers on the difficulty of the factoring problem. —Ed.)

ABSTRACT

Here are the results of some simple estimations I have done on the projected difficulty of factoring various sizes of numbers for the next 25 years.

The basic question is:

> "In the year YYYY, what size number will I be able to factor for an investment of $DDDD?"

To be specific, I've looked at

YYYY= 1990, 1995, 2000, 2005, 2010, 2015
and
$DDDD = $25K, $25M, and $25G

(that is, $25,000, $25,000,000, and $25,000,000,000). The three levels might correspond to "individual", "corporate", and "national" levels of attack. All calculations are done in 1990 dollars.

Each of these estimates is also done in an "high," "average," and "low" point of view. (That is, the high estimates are for the greatest number of digits possible, while the low estimates are for the least number possible.)

The estimates are done in terms of MIP-years, a computational unit of power analogous to a "kilowatt-hour" of electricity. Specifically, a MIP-year is the computational power of a one-MIP machine running for one year. A MIP (more correctly, a MIPS) is a "million-instruction per second" machine. Today's workstations run in the 1 to 10 MIPS range, and 100 MIPS machines are under development. One MIP-year corresponds to 3.15×10^{13} operations.

FACTORING ALGORITHMS

To factor a number n with current technology using the best known algorithms, we need a number of operations roughly equal to

$$L(n) = \exp\left(\sqrt{\ln n \ln \ln n}\right) \qquad (1)$$

(Using, say, the quadratic sieve algorithm.)

continued on page 8

RSA Factoring Challenge Update

The RSA Factoring Challenge, sponsored by RSA, is essentially a list of very long numbers posted on the RSA host on the Internet (rsa.com). The Challenge serves two purposes: it provides a testing platform for new factoring algorithms, and it also provides data which RSA (and others) use to measure the advance of factoring technology. RSA then turns around and uses these data to recommend key sizes for various customer projects, based on the customer's security needs.

The numbers in the factoring challenge are of two types; so-called *partition numbers*, which can act as a good general assessment of factoring algorithms, and RSA *challenge numbers* which are numbers of the type that would typically be used as RSA moduli, because they are assumed to be particularly difficult to factor.

There are cash prizes for the most successful factorers, although the rules by which the money is distributed ensure that factoring a smaller partition number that has remained unfactored for a relatively long time is rewarded more than the factoring of a larger partition number. Factoring any RSA challenge number is a considerable achievement in itself, and is rewarded accordingly. Prizes vary anywhere from the tens to the thousands of dollars, and unrewarded prize money rolls over in a "kitty" from month to month, much like a State Lottery.

continued on page 10

RSA Laboratories Report

Over recent months, RSA Laboratories has become increasingly busy. As well as the customary work of technical support and independent consulting, we continue to maintain our close awareness of recent work in the cryptographic community, particularly new results from recent IACR meetings such as Eurocrypt '93. We are releasing an increasing number of RSA Laboratories technical reports and we anticipate the imminent publication of the newly updated version of "Frequently Asked Questions".

New projects have included an analysis of the vast quantity of data received as a result of the RSA Factoring Challenge. The challenge was established over two years ago with the aim of assessing the limits in factoring ability. A full analysis of this data is now being concluded and the full report will be available soon.

A particularly exciting development has recently become a major research priority at the Labs. Research at RSA Laboratories has revealed a cryptographic technology that could provide a solution to some of the more pressing problems associated with the distribution of data by CD-ROM. Patent applications have been filed, and the project code-named "Arcade".

Recently we were pleased to host our first annual RSA Laboratories Seminar Series. Diverse sessions provided not only a full review of many of today's issues, but also news and assessment of the very latest advances within the cryptographic community. We are pleased to report that there was considerable interest in this new venture, with scientists and developers from many of our major licensees attending. Currently, of course, we are quite busy planning technical sessions for January's upcoming 1994 RSA Data Security Conference – we hope to see you there!

— Dr. Matthew Robshaw

We use this formula for our "low" estimates, since this is currently achievable. For our "average" estimate, we use the formula

$$A(n) = \min(L(n), \exp(2.08 (\ln n)^{1/3} (\ln \ln n)^{2/3})) \quad (2)$$

This presupposes that the number field sieve (NFS) can be generalized to handle ordinary (cryptographic) numbers, as conjectured in the 1990 ACM STOC article. Finally, for the high estimates, we use the formula

$$H(n) = \exp(1.526 (\ln n)^{1/3} (\ln \ln n)^{2/3}) \quad (3)$$

which is the number of operations that NFS now uses for rarefied numbers. (Achieving this formula would be quite a breakthrough.)

COSTS OF COMPUTATION

I estimate that today a MIP-year costs about $10, as follows. You can buy (parts for) a 10-MIP machine for about $500. With a lifetime of five years, you get 50 MIP-years out of the machine.

As for rates of technological progress, for the "low" estimate I assume that technology only advances at 20%/year. For the "average" estimate I assume that technology advances at 33%/year, and for the "high" estimate I assume 45%/year. These are measured in terms of the drop in the cost of a MIP-year in constant 1990 dollars. Thus, under the high estimate, $10 will buy 1.45 MIP-years in 1991 and 2.10 MIP-years in 1992, etc.

At this rate, we can estimate the number of MIP-years that can be bought for $1 as follows:

Year	Low	Average	High
1990	0.100	0.100	0.100
1995	0.249	0.416	0.641
2000	0.619	1.732	4.109
2005	1.540	7.207	26.340
2010	3.833	30.000	168.800
2015	9,540	124.800	1082.000
2020	23.74	519.500	6935.000

Combining this with our "low" ($25K), "average" ($25M), and "high" ($25G) estimates for dollars available, we arrive at the following chart for the number of MIP-years affordable. (Here T is the abbreviation for "tera," i.e. 10^{12}.)

Year	Low	Average	High
1990	2.5K	2.5M	2.5G
1995	6K	10M	16G
2000	15K	43M	103G
2005	38K	180M	658G
2010	96K	750M	4.2T
2015	239K	3.1G	27T
2020	549K	13G	173T

That is, in the year 2020, a determined opponent with $25G might be able to afford 173 tera MIP-years to attack a number.

RESULTS

We now give the number of operations required to factor numbers of various sizes under our low, average, and high estimates (formulas (1), (2), and (3)). These are in MIP-years.

Digits	Low	Average	H
100	74	74	0
150	1M	1M	3
200	4G	4G	4
250	6T	2T	26
300	5×10^{15}	3×10^{14}	1(
350	2×10^{18}	2×10^{16}	25
400	9×10^{20}	10^{18}	5
450	2×10^{23}	6×10^{19}	8
500	4×10^{25}	2×10^{21}	1

Combining the above charts with additional calculation, we end up w low, average, and high estimates size of a number (in digits) that an a would be able to factor at various pc time.

Year	Low	Average	H
1990	117	155	3
1995	122	163	4
2000	127	172	4
2005	132	181	4
2010	137	190	5
2015	142	199	5
2020	147	204	6

CONCLUSIONS

If one wishes to devise a "standard" on a 25-year lifetime for an average then a recommendation of 200 d digits (665 bits) seems justified. A " master" key over the same lifetime well be chosen to be three times that (600 decimal digits, or 1994 bits).

— Dr. Ron

Arkhon *Continued from page 4*

Arkhon has joined together with the preeminent system software vendors in the industry, including companies such as RSA, Oracle and OCSG. Sometimes called a "virtual corporation", such partnerships allow a group of specialized companies to combine their expertise synergistically to create products with complex functionality in a more timely fashion than traditional software producers.

Arkhon's architecture allows the modular incorporation of any required system or application software, providing to the user a single programming interface and a consistent look and feel. Additionally, Arkhon offers consolidated support, trainir line documentation, and tutorial so for its full product line. Arkhon a partners constitute the only virtual ration with complex solutions to the lems of enterprise management. C Arkhon at 310/809-0760.

— Stan Tomsic, Arkhon Techr

The attached images are scanned from the fall 1993 Cyphertext newsletter put out by RSA Data Security Inc and are (C) Copyright 1993 RSA Data Security Inc.

RSA has given me permission to put them on the net and for everyone to make hardcopy reprints, provided they are copied in entirety.

RSA expects to put a postscript version of the paper (not scanned) on rsa.com and www.rsa.com later this month.

This file is ftp://furmint.nectar.cs.cmu.edu/security/rivest-factoring.ps.Z

Vince Cate
5/4/94