Noesis

The Journal of the Hoeflin Research Group

(Issue 34, January 1989)

Editorial

Ronald K. Hoeflin
P.O. Box 7430
New York, NY 10116

Editorship of "Noesis": If no one volunteers to edit Noesis starting with issue 37 (April 1989), I will reduce the publication schedule from monthly to quarterly (4 times a year).

Richard May: Member Richard May indicates that he is listed in the 22nd edition of Who's Who in the East, 1989-1990. He says that he has mentioned the Hoeflin Research Group in his biographical sketch, which appears on page 564.

> **MAY, RICHARD WARREN,** author, inventor, educator; b. Marlboro, Mass., Mar. 1, 1944; s. Richard and Lavinia (Crane) M. BS in Psychology, U. Mass., 1968. Lic. real estate broker. Tchr. Boston Pub. Schs., Boston, 1970—; pres., founder The Aleph (formerly Prometheus Pastimes), Boston, 1975—; adv. bd. mem. and research assoc. Point One Adv. Group, Inc. Author: (games of strategy) Game of the Gods, 1984, TriHex, 1985; patentee game bd. and pieces TriHex, 1988. Mem. Assn. Advance Ethical Hypnosis, West Orange, N.J., 1974-75, Boston Tchrs. Union, 1984—. Sr. fellow Internat. Soc. Philos. Enquiry (sr., asst. historian 1981-82); mem. Prometheus Soc. (charter editor ombudsman 1984—), Hoeflin Research Group, Triple Nine Soc. (membership officer 1983-84, regent 1987—), Mensa, Club Intertel (Lakewood, Colo.).

Members: In this issue I list the 17 members of the Hoeflin Research Group as well as the 16 members of the Mega Society. Of our 17 members I have met 7: Cole, Hajicek, Inada, May, Raniere, vos Savant, and Wise. Of the 16 Mega Society members I have met 6: Alger, Bloom, Egendorf, Langdon, Van Vleck, and vos Savant. I have not been affiliated with the Mega Society since 1985, so the list of its members is courtesy of S. Woolsey.

Societies: In this issue I also list eleven high-IQ societies. Seven of them accept scores of my Mega Test for admission purposes, as indicated on the list. I have been a member of seven of the groups at one time or another: Mensa, Intertel, Triple Nine, I.S.P.E., Four Sigma, Prometheus, and Mega. I am the founder of Prometheus, the Hoeflin Research Group, and Mega and co-founder of Triple Nine. I currently belong to just two of the groups, Mensa and Triple Nine, but I plan to withdraw from Triple Nine shortly.

International Directory of Distinguished Leadership: I am supposed to be listed in this biographical directory in its 1990 edition. I am not sure that this reference work is widely available in libraries, although it claims to be, I believe.

More odd words--a mini-"Pop Quiz": As a supplement to my quiz in an earlier issue of Noesis that asked whether certain words can be found in Webster's Ninth New Collegiate Dictionary, I pose the question which of the following words and phrases can be found in that dictionary: jillion (meaning a very large number a la zillion), spaghetti western, hunky-dory, jeepers creepers, beaver (meaning the female pudenda).

Issue 8: I still have not yet reduced issue 8 of this journal to this smaller size, as I did with the first seven issues, due mainly to its great length (24 pages). But you will each receive a reduced-size copy eventually.

Members of the Hoerlin Research Group

Ronald K. Hoerlin
P.O. Box 7430
New York, NY 10116

The following is a list of current members of the Hoerlin Research Group, including a new address for Richard May. Of these 17 members, 3 are also members of the Mega Society: H. W. Corley, Marilyn vos Savant Jarvik, and Jeff Ward. If there are any errors below, e.g., the omission of an M.D. or Ph.D., please let me know. See the following page for a list of Mega Society members.

Geraldine Brady
5728 S. Blackstone Ave., Apt. 210
Chicago, IL 60637

Anthony J. Bruni, Ph.D.
112 Harvard Ave., Apt. 81
Claremont, CA 91711

Chris Cole
P. O. Box 9545
Newport Beach, CA 92658

H. W. "Bill" Corley
626 Charles Court
Arlington, TX 76013

Eric Erlandson
2051 Worthington Ave.
Lincoln, NE 68502

James D. Hajicek
5894 Spring Valley Road
Burlington, WI 53105

Eric Hart
P. O. Box 813
Miller Place, NY

Dean Inada
23333 Ridge Route Drive, Apt. 51
El Toro, CA 92630

G. M. Langan
P. O. Box 131
Speonk, NY

Richard May
53 Hancock Street, Apt. 5
Boston, MA 02114

Johann Oldhoff
Hagalundsg. 37 VI
S-17151 Solna
Sweden

Keith Raniere
3 Flintlock Lane
Clifton Park, NY 12065

Cedric Stratton, Ph.D.
P. O. Box 60111
Savannah, GA 31420

Marilyn vos Savant Jarvik
124 West 60 Street, Apt. 39S
New York, NY 10023

Jeff Ward
13155 Wimberly Square, Apt. 284
San Diego, CA 92128

Ray Wise
48 Winthrop Street
Torrington, CT 06790

Karl G. Wikman
Åsklostervägen 41
430 21 Åskloster
Sweden

The Question

9,412,343,607,359,262,946,971,172,136,294,514,357,528,981,378,983,082,541,347,532,211,942,640,121,301,590,698,634,089,611,468,911,681

The Answer

86,759,222,313,428,390,812,218,077,095,850,708,048,977 × 108,488,104,853,637,470,612,961,399,842,972,948,409,834,611,525,790,577,216,753

A Most Ferocious Math Problem Tamed

By MALCOLM W. BROWNE

By piecing together the output of hundreds of computers on three continents, a team of mathematicians succeeded yesterday in solving a monster computational problem that had defied all previous efforts. The achievement is likely to force cryptographers to reassess the future application of some codes used by governments and banks.

At 2:03 A.M., Pacific daylight time, the last sequence of numbers required for the solution popped up in a computer laboratory in Palo Alto, Calif., and news of the triumph was flashed to collaborators around the world. The team had succeeded for the first time in splitting a number 100 digits long into two large, prime factors.

The factors of a number are smaller numbers which, when multiplied by each other, yield the larger number. A prime number is one that is evenly divisible only by one or by itself. The prime factors of 15, for example, are 3 and 5.

Maximum Possible Difficulty

The two factors found for the 100-digit number, which was selected by an elaborate mathematical screening process to pose the maximum possible difficulty, are respectively 41 digits and 60 digits long.

The organizers of the project were Dr. Mark S. Manasse of the Digital Equipment Corporation's Systems Research Center in Palo Alto and Dr. Arjen K. Lenstra of the University of Chicago. But a dozen users of some 400 computers in the United States, the Netherlands and Australia were recruited to join in the project, donating computing time from intervals when the computers were not needed for their regular work.

Several of the most secure cipher systems invented in the past decade are based on the fact that large numbers are extremely difficult to factor, even using the most powerful computers for long periods of time. The accomplishment of factoring of a 100-digit number "is likely to prompt cryptographers to reconsider their assumptions about cipher security," Dr. Lenstra said in a telephone interview.

His colleague, Dr. Manasse, added: "What this shows is that a cryptographer should avoid basing a cipher on any factorable number smaller than about 200. The cipher system still works, but we have upped the ante." Using larger numbers makes the work of cryptographers more cumbersome and time-consuming.

One cryptographic system based on the difficulty of factoring large num-

bers was invented in 1977 by Ronald L Rivest, Adi Shamir and Leonard Adelman, all of the Massachusetts Institute of Technology. The three mathematicians patented their system and now market computer chips especially designed to apply it. In this and similar systems, digits replace each letter in a text message, and the entire sequence of digits is treated as a single large number. A mathematical operation is then performed on this number, and to decipher the result requires either that the receiver possesses the key or breaks the code by factoring the large number.

This kind of cipher system is regarded as too slow and cumbersome for such routine cipher messages as those used for secret government messages and the transfer of funds between banks. But according to Dr. Ron Graham, a mathematician at A.T.&T. Bell Laboratories, the "RSA System" (which takes its initials from the names of its inventors) is used fairly extensively for the secure transmission of encryption and decryption keys from one organization to another.

Guarding Secret Keys

Encryption and decryption keys must be protected more securely than any other secret message, because these are the keys that allow either the intended recipient of a cipher message or a spy to decipher it. Since such a key is relatively short, the slowness of encrypting and decrypting it is a disadvantage more than offset by the method's relative security.

The RSA method can accommodate factorable numbers of virtually any length as cipher keys, so yesterday's achievement does not compromise the method itself.

"Even if a user were to adopt a key 100 digits long," Dr. Manasse said, "it would take a gigantic organization working with single-minded dedication to accomplish what our network has done. I doubt that any organization using this kind of cipher is seriously worried by what we have done."

Theoretically, a costly supercomputer such as the Cray, operating continuously, could have solved the problem in about one week, an expert said. But running such supercomputers costs many thousands of dollars an hour. By operating many simpler computers, when they were idle for a few minutes or hours, the problem was solved at virtually no cost.

Progress toward factoring a 100-digit number has been rapid this year, even though no new methods of factoring have been developed. Just three weeks ago, the same group led by Dr. Manasse and Dr. Lenstra established another record by factoring a number 96 digits long, and last spring, a Netherlands mathematician, Herman te Riele, factored 92 digits. In the 1980's the record has been broken about once a year, Dr. Lenstra said.

Technique Is Not New

Dr. Andrew M. Odlyzko, a mathematician at A.T.&T. Bell Laboratories in Murray Hill, N.J., said that the basic technique used for the calculation was not new.

The algorithm, or computer method, the team applied ,"which is called the 'quadratic sieve,' was invented some years ago by Dr. Carl Pomerance of the University of Georgia at Athens," Dr. Odlyzko said. "In a way, it's slightly disappointing that we have not come up with any real advance over that method in factoring large numbers. There are a lot of variations of the same general method, but they are all roughly equal in efficiency."

The great advantage of the quadratic sieve is that it enables its user to break an enormously complex computational problem down into a large number of relatively simple computations. Each of these computations can be carried out independently and in any sequence.

The strategy, Dr. Lenstra explained, is to calculate a "matrix" of numbers, a square consisting of 50,000 rows and 50,000 columns, in each of which is a number that contributes some information about the solution of the problem. Ideally, a computer could be assigned to calculate each square in the matrix, but in this case, only about 400 computers were available.

"In any case, however," Dr. Manasse said, "we approached the problem as a massively parallel computation, one in which many processors were working along parallel lines simultaneously. As each small task was completed, the computer user would send us the result by electronic mail.

"Last weekend, we realized that we had enough of these preliminary computations to put them together, using a technique called Gaussian elimination. That gave us the final result last night," he said.

Gaussian elimination is a procedure analogous to the elimination of vari-

ables in an algebraic expression by canceling out like values.

Dr. Manasse said that the factoring program had attracted the interest of mathematicians and computer scientists in Canada, West Germany and other countries, and that many had volunteered to participate in a continuation of the program.

Next: 106 Digits

The factoring of a 100-digit number took less than one month, and the pace is likely to continue. "By the end of the winter I would expect that we will have factored a number of 106 digits," Dr. Manasse said.

Asked whether mathematicians had sighted new factoring techniques that might speed the process, he replied: "I'm not anxious to see any radically new techniques emerge. Of course, if they're out there, we'll have to use them. But I would like to see the RSA encryption system continue as a secure safeguard."

All encryption systems are under the continuous scrutiny of the National Security Agency, the Federal agency chiefly responsible for safeguarding American ciphers and cracking the ciphers of other nations. Experts from the agency attend meetings of mathematicians and computer scientists and follow academic developments closely.

"It's a safe bet that the N.S.A. knows all about what we've done," Dr. Manasse said, "although we've had no communication from them. In any case, this is not going to give them nightmares. It may just make the code makers a little more cautious. We've done something that once would have been regarded as practically impossible."

NEW YORK POST, THURSDAY, NOVEMBER 17, 1988

Tue takes learning to the nth degree

BOSTON (AP) — Tue Nguyen did more than nibble from the tree of knowledge — he made a feast of it.

Nine years after arriving in the U.S. with thousands of other Vietnamese boat people, Nguyen, 26, has earned his seventh degree from the Massachusetts Institute of Technology — a doctorate in nuclear engineering.

The school says the seven degrees are an MIT record.

The super scholar, now a nuclear physicist, is preparing to start a job at IBM, designing technology for the manufacture of semiconductor devices.

"You're not likely to find another person like this very often," said nuclear engineering professor Sidney Yip, Nguyen's MIT doctoral adviser.

"He's a very quiet guy, very laid back," said Yip. "But, as you can imagine, deep down he has a lot of willpower."

Nguyen entered MIT in 1981.

By taking up to 12 courses a semester, instead of the normal student load of four, he earned his first undergraduate degree in three years and finished four additional bachelor's degrees in one year more.

He then began graduate work.

He holds bachelor's degrees in physics, computer science and engineering, electrical engineering, mathematics and nuclear engineering.

He earned his master's degree in nuclear engineering in 1986 and finished work on his doctorate this fall.

He also studied English in Texas and went to Harvard for Chinese, the language of his fiancee's family.

Nguyen and two younger brothers fled Vietnam in 1978, leaving their father — a retired government employe — and mother behind with two other sons and a daughter.

After three days at sea in a small boat with 300 refugees, the brothers arrived in Malaysia and spent nine months in a refugee camp before coming to the U.S.

His brothers have done almost as well as he has.

Tien Nguyen, 25, is earning a doctorate in nuclear engineering at MIT, and Tai Nguyen, 22, is doing graduate work at the University of California, Berkeley.

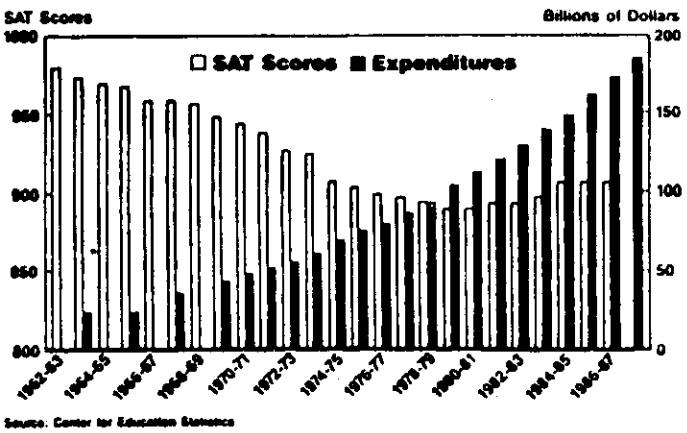
TUE NGUYEN

While Nguyen has "a great deal of scientific curiosity," Yip said he worries about him:

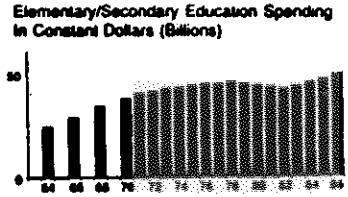
"He has, in some sense, not really known the outside world. He spent most of his time in an academic environment."

THE NEW YORK TIMES. SUNDAY. SEPTEMBER 4, 1988

Elementary/Secondary Education Spending and Achievement: 1963-1988



Source: Center for Education Statistics



Members of the Mega Society

Donald K. Hoefflin
P.O. Box 7430
New York, NY 10116

S. Woolsey sent me the following list of members of the Mega Society from the fall 1988 issue of that group's journal. I have added the addresses from the January 1989 issue of that journal, in case any of you wish to communicate with members of that group. If any of these addresses are wrong, you might ask S. Woolsey, Jeff Ward, or some other Mega member for an updated address.

Ferris Alger
Old York Road, Route 3
New Hope, PA 18938

Phillip Bloom
140 Cadman Plaza west, Apt. 3-F
Brooklyn, NY 11201

H. W. "Bill" Corley, Ph.D.
626 Charles Court
Arlington, TX 76013

Robert Dick
13 Speer Street
Somerville, NJ 08876

Andrew Egendorf
P. O. Box 646
Weston, MA 02193

Christopher Harding
P. O. Box 5271
Rockhampton Mail Centre
Queensland 4702
Australia

Kevin Langdon
P. O. Box 795
Berkeley, CA 94701

John McAdon
8024 Southside Blvd., Apt. 174
Jacksonville, FL 32216-8023

Donald O'Brien
10864 Alderbrook Lane
Cupertino, CA 95014

Carl J. Porceny, M.D.
3630 Winding Creek Way
Winston-Salem, NC 27106

Avrom A. Rosen
4100 west 100 Terrace
Leawood, KS 66207

Edgar M. Van Vleck
174 Frederick Court
Los Altos, CA 94022

Johannes D. Veldhuis, M.D.
105 Vincennes Road
Charlottesville, VA 22901

Marilyn vos Savant Jarvik
124 west 60 Street, Apt. 39S
New York, NY 10023

Jeff Ward
13155 Wimberly Square, Apt. 284
San Diego, CA 92128

S. Woolsey
P. O. Box 1942
Houston, TX 77251

High-IQ Societies

Ronald K. Hoeflin
P.O. Box 7430
New York, NY 10116

The following is a list of the eleven extant high-IQ societies with which I am acquainted, along with their percentile cut-offs and their addresses. All have monthly journals except the Geniuses of Distinction Society, which has no journal, the Cincinnatus Society, which I am told publishes 4 times a year, the Four Sigma Society, which purports to publish 4 times a year but probably does not publish that frequently, and the Mega Society, which publishes monthly up to 1985 but subsequently has published only 3 times, to my knowledge. Those groups marked (+) accept my Mega Test for admissions.

Mensa, 98th percentile, American Mensa, Ltd., 2626 East 14th Street, Brooklyn, NY 11235

Intertel, 99th percentile, P. O. Box 15580, Lakewood, CO 80215

(+) Geniuses of Distinction Society, 99.6th percentile, c/o Anton Montalban-Andersson, P. O. Box 3434, Center Line, MI 48015

(+) Cincinnatus Society, 99.9th percentile, c/o Grady Ward, 380 N. Bayview Ave., Sunnyvale, CA 94086

Minerva Society, 99.9th percentile, c/o Jalon Leach, 11526 Tina St., Norwalk, CA 90650

(+) Triple Nine Society, 99.9th percentile, c/o Barry Kington, P. O. Box 1111, Madisonville, KY 42431

(+) International Society for Philosophical Enquiry, 99.96th percentile (99.9 on a test like the Mega Test plus 99.9 on the ISPE's own vocabulary test), c/o Donna Kopp, 5040 Cliffhaven Drive, Annandale, VA 22003

Four Sigma Society, 99.997th percentile, c/o Kevin Langdon, P. O. Box 795, Berkeley, CA 94701

(+) Prometheus Society, 99.997th percentile, c/o Robert Dick, 13 Speer St., Somerville, NJ 08876

(+) Hoeflin Research Group, 99.9995th percentile, c/o Ronald K. Hoeflin, P. O. Box 7430, New York, NY 10116

(+) Mega Society, 99.9999th percentile, c/o Jeff Ward, 13155 Wimberly Square, Apt. 284, San Diego, CA 92128