Reprinted from
Notices of the American Mathematical Society
Volume 30, Number 1, January 1983

Primes, Codes and the National Security Agency

Susan Landau

Physicists lost their innocence and freedom from government controls with Los Alamos. For biologists that time came in 1976 with National Institutes of Health regulation of recombinant DNA experiments. Mathematicians have been free from restraint—until now. The National Security Agency (NSA) has asked for and received an agreement of prior review on articles concerning cryptography. It recently sought to fund proposals for research in computational mathematics submitted to the National Science Foundation (NSF). Mathematics rarely makes the headlines, but the article on the front page of *The New York Times* of August 27, 1980 was startling—"Science Agency Blocks Funds to Aid Research on Computer Coding." Even more surprising is that the NSA is funding research on factoring integers. Factoring is so basic a problem that schoolchildren are asked to do it; how could it be a threat to national security?

The interest stems from the crucial role that primes and factoring play in a new mathematical cryptographic scheme. For centuries cryptography was the domain of the military, but an increasing reliance on computer data banks for anything from medical histories to credit records has changed that. There is a growing need for secure transmission of data which has made cryptography an active area of research in the private sector. The critical component of the sending of secret messages is a secure cipher. If many messages using the same code are intercepted, the cipher may be discerned by knowing the frequency distribution of letters in the language. Frequent changes of the cipher removes this problem, only to raise another: how to transmit the encryption scheme securely?

Seeking a way out of this dilemma, Whitfield Diffie and Martin Hellman of Stanford and Ralph Merkle of Berkeley proposed Public-Key cryptography in 1976. In short, Diffie, Hellman and Merkle envisaged an encryption mechanism in which even if the encryption method were known, decryption would be difficult and take years. By the time intercepted messages could be unraveled, the information would be outdated and useless. Encryption would be a "trapdoor"; its strength would lie in the inherent infeasibility of certian computations. At the time of Diffie and Hellman suggested several possibilities for such schemes but saw no workable method. Three computer scientists then at MIT, Ronald Rivest, Adi Shamir and Leonard Adleman did. They had a clever idea to exploit the contrast between the speed of primality testing and the apparent difficulty of factoring. Multiplying together two large primes would be a trapdoor from which factoring would be the exit.

SUSAN LANDAU is a doctoral candidate at the Massachusetts Institute of Technology in applied mathematics and computer science. Her thesis, under the supervision of Gary L. Miller, presents a polynomial time algorithm for testing solvability by radicals; her research interests include algebra and theoretical computer science. She has taught for five years at Hampshire College Summer Studies in Mathematics, an NSF program for high ability high school students.

The groundwork for their scheme had been laid in the early seventies. While logicians have wrestled for decades with the question of decidability, the issue in computer science instead has been complexity: on a problem of input size "m", how many steps does it take as a function of m to solve the problem? Answers to this question involve obtaining algorithms which provide an upper bound on the complexity of the problem, and lower bounds which show that any conceivable algorithm will require a certain number of steps. Exhibiting lower bounds is hard; for example, the present best lower bounds on the complexity of multiplying two $m \times m$ matrices is $O(m^2)$ (an obvious bound since there are m^2 entries), while the best algorithm is $O(m^{2.496})$.

The critical distinction comes between problems with polynomial time algorithms, and those which require exponential running time. The compexity of factoring integers is unknown, but best present factoring algorithms work in $m^{1.6(m/\log m)^{1/2}}$ steps on an integer of m digits, which means that factoring a random one hundred digit number is essentialy infeasible. Primality testing would appear to be as difficult, but in 1974 Gary Miller of Berkeley devised an algorithm which uses the Extended Riemann Hypothesis (ERH) to test primality of an m digit integer in $O(m^4)$ steps. ERH guarantees the existence of a quadratic non-residue less than $O(\log^2 p)$ in $\mathbf{Z}/p\mathbf{Z}$, which Miller's algorithm needs to check primality. An approach which avoids the use of ERH was found by Robert Solovay of IBM and Volker Strassen of the University of Zurich; theirs is a probabilistic algorithm which tests primality of an m digit integer in $O(m)$ steps. If the integer

to be checked is prime, the Solovay-Strassen test responds "prime"; if the integer is composite, with probability no greater than one-half, the test declares it to be prime. Suppose a is an integer less than n, which is relatively prime to n; and let (a/n) be the Jacobi symbol of a on n. If n is prime, then $(a/n) \equiv a^{(n-1)/2} (\mathrm{mod}\, n)$. Solovay and Strassen noted that the set $\{a | (a/n) \equiv a^{(n-1)/2} (\mathrm{mod}\, n)\}$ is a proper subgroup of $(\mathbf{Z}/n\mathbf{Z})^*$ for composite n. This means that at least half the a's less than n and relatively prime to n do not satisfy $(a/n) \equiv a^{(n-1)/2} (\mathrm{mod}\, n)$. The Solovay-Strassen test computes (a/n) (by quadratic reciprocity) and $a^{(n-1)/2} (\mathrm{mod}\, n)$; if the two are not equal, the test responds "composite," otherwise it calls the integer "prime." The algorithm runs k independent trials; if any respond composite, the integer is composite, and is discarded. If all the trials say the integer is prime, then the probability that it is composite is less than $1/2^k$. Since Miller's algorithm depends on ERH, and the Solovay-Strassen procedure is probabilistic, the existence of a polynomial time algorithm for testing primality remains an open question. In 1980 however, Adleman, Robert Rumely, then at MIT, and Carl Pomerance of the University of Georgia developed a subexponential algorithm; their test runs in $O(m^{c \log \log n})$ steps on an m digit integer, where c is a constant. The upshot of these results is that within fifteen seconds a computer can check primality of a fifty-digit number.

The MIT group used the contrasts in complexity to create a simple and elegant Public-Key system. Each participant in the cryptosystem finds two large primes $(\sim 10^{50})$ p and q by one of the fast primality algorithms. Let $n = pq$, and let $\varphi(n)$ be the Euler phi-function of n. Each participant also chooses an "a", an integer which is less than n and which is relatively prime to $\varphi(n)$: such an integer can easily be found since most integers less than n are relatively prime to $\varphi(n) = (p-1)(q-1)$. Thus choose a less than n and test whether $(a, \varphi(n)) = 1$; if not, repeat until an a which satisfies the conditions is found. The Public-Key book prints each participant's n and a. Suppose the Bank of England wants to communicate with the Federal Reserve. The Bank of England would proceed as follows:

1) Translate the message into numbers, say A = 01, B = 02, etc.

2) Break the message into blocks of convenient size.

3) Consult the Public-Key book for the recipient's n and a.

4) Send each *block* as $(block)^a (\mathrm{mod}\, n)$.

Decryption is simple for the recipient. Since $(a, \varphi(n)) = 1$, there exist x and y such that $ax + \varphi(n)y = 1$, and x and y can be quickly computed from a and $\varphi(n)$. The Fed would decode as follows:

1) Break the message up into blocks.

2) For each *block*, compute $(block)^x (\mathrm{mod}\, n)$.

3) Glue the blocks back together

4) Decode by 01 = A, 02 = B etc.

This yields the original message, since

$$\begin{aligned} (block^a)^x &\equiv (block)^{ax} \\ &\equiv (block)^{1-\varphi(n)y} \\ &\equiv (block)\,(\mathrm{mod}\, n), \end{aligned}$$

Euler's

by ~~Fermat's Little~~ Theorem. The Fed decodes the communication easily, since it takes polynomial time to compute x given $\varphi(n)$. An interceptor of the communication could do exactly the same calculation, except that he knows n, not $\varphi(n)$. The standard way to compute $\varphi(n)$ is to factor n, and in fact, Miller has shown that calculating $\varphi(n)$ is polynomial time equivalent to factoring n. Since n is the product of two fifty-digit primes, it is infeasible to factor it using best known algorithms.

Rivest, Shamir and Adleman announced their result in April 1977. The public became aware of it when Martin Gardner described the system in his Mathematical Games column of the August 1977 *Scientific American*. The discovery also attracted attention from other circles. Shortly before Rivest was scheduled to present the work at an Institute of Electrical and Electronics Engineers (IEEE) conference in Ithaca, New York, the IEEE received a letter from one J. A. Meyer of Bethesda, Maryland, warning that publication of cryptography results might be in conflict with the 1954 Munitions Control Act which regulated the flow of weapons and sensitive equipment to foreign countries. Meyer also said that dissemination of the conference proceedings abroad might be illegal. On the advice of the MIT lawyers, Rivest suspended sending out preprints.

A reporter from *Science*, Deborah Shapley, soon discovered that Meyer was listed as an employee of the National Security Agency. The NSA denied involvement with the letter, and a spokesman claimed that J. A. Meyer had written it as a private citizen. Rivest, Shamir, and Adleman decided to present their results at the conference and to resume mailing of their paper.

Nothing was heard from the NSA for a year and a half, until a speech by its Director, Admiral Bobby Inman, in 1979. He said that open publication of research in cryptography was harmful to the national security because it interfered with the NSA's abiltiy to gather and protect intelligence, and urged that a dialogue between the NSA and the academic community begin. The American Council on Education proposed the formation of the Public Cryptography Study Group (PCSG), with eight members from the academic community (the majority of them mathematicians and computer scientists), and one member from the NSA, Daniel Schwartz, a lawyer.

In a series of meetings during 1980-1981, the NSA argued for voluntary agreement regarding

publication of cryptography research. The agency claimed that academic work might inadvertantly compromise United States encryption schemes. Research on the weaknesses of cryptosystems might also lead foreign governments to adopt more sophisticated systems, thus denying the U.S. needed intelligence. Although it preferred a voluntary agreement, the NSA made clear that it was also considering seeking statutory authority for prepublication review of sensitive material. (As precedent, the NSA cited two Federal laws: the Arms Export Control Act (22 U.S.C. 2778), which restricts foreign dissemination of certain information relating to cryptology and supercedes the 1954 Munitions Control Act, and Section 181 of Title 35 U.S.C. which permits the imposition of a secrecy order upon a patent application when issuance of a patent would be harmful to national security. Since algorithms and scientific papers are not patentable, neither related to domestic release of nongovernmental research in cryptography.) On January 5, 1981, the PCSG approved a two-year experiment under which the NSA would inform the academic community of its interest in reviewing cryptography papers prior to publication. Compliance would be voluntary, and review prompt. If the NSA wanted to delete portions of a paper, or prevent publication, it would first consult with an advisory panel (whose members would have top security clearance), although the NSA would not be bound by the decisions of the advisory group. Changes would be explained to the greatest degree possible.

One committee member, George Davida, professor of computer science at the University of Wisconsin, issued a dissenting report. He argued that the NSA's attempt to control publication of cryptography research was of questionable legality, and he called attention to a memorandum the Justice Department had issued stating that, "It is our view that the existing provisions of the ITAR [International Traffic in Arms Regulation of the Arms Export Control Act] are unconstitutional insofar as they establish prior restraint in disclosure of cryptographic ideas and information developed by scientists and mathematicians in the private sector." Davida contended that the risks to the NSA were far outweighed by the benefits to the public, and that the direction and quality of research in cryptography would be seriously affected by the withholding of results. Rather than limit public research, the NSA should "perform its mission in the old-fashioned way: stay ahead of others," Davida bluntly suggested.

The situation grew more serious in August 1980 with the renewal of Leonard Adleman's NSF grant. His budget had already been renegotiated when Adleman was informed that the NSF would be unable to fund part of it due to "national security reasons." NSF would support Adleman's work on the complexity of number-theoretic problems and on VLSI (chip design), but declined to support his research in cryptography or related problems. Shortly afterwards Adleman received a call from Admiral Inman, who offered that the NSA fund Adleman's work. Because NSF funds are limited, the procedure has always been that if a mission agency was interested in funding a proposal, it would do so instead of NSF. The issue here though was disclosure; if the NSA supported Adleman's research, might it classify it?

On October 9, 1980 representatives from the NSA and the NSF met with White House science advisor Frank Press to clarify the issue. The decision was made that both agencies would fund cryptography research for the present. Although the NSA would require investigators it supports to submit articles to the agency prior to publication, it would not expect to classify the research it supported. Adleman was offered the choice of NSA or NSF funding; he accepted NSF support because, "On a personal level I saw myself as a pure scientist and my natural affinities were to be funded by NSF. As a scientist, it was clear that there would be a national debate on the issues and I didn't want any action I might take to be misconstrued as suggesting that the NSA had a compelling case that they had a role to play in the scientific process."

Subsequent to this, a subcommittee of the NSF Mathematics and Computer Sciences Advisory Subcommittee was convened to discuss NSF's role in supporting cryptology research. On July 13, 1981, it issued its report, which stressed the importance of cryptology to business and private citizens. "Tampering with information related to such things as electronic funds transfers ... is a new threat which can be posed by criminal, terrorist or enemy agents to personal, corporate or national security ... it is clear that increased computerization of our society is leading to the accumulation of vast amounts of personal information ... it is imperative that steps be taken to limit access to this information," the report said. The panel expressed concern that NSF's budget limitations might soon lead the NSA to dominate the field of cryptography, and recommended that the NSF encourage the Department of Commerce to fund research in this area. The Public Cryptography Study Group guidelines came in for sharp criticism. "The proposed system of prepublication review is unnecessary, unprecedented, and likely to cause damage to the ability and willingness of American research scientists to stay at the forefront of research in public sector uses of cryptology." Finally, the NSF report observed that cryptography is no more of a threat to national security than many areas of basic research, but that it was distinguished by the fact that a single government agency had controlled the area for nearly thirty years.

Davida and others argue that national security is imperiled more by the lack of secure encryption systems in the commercial environment than

it is by the knowledge garnered by foreign powers from the publication of cryptography research. There can be little doubt of the importance of cryptography to industry, business, banking, and the Department of Commerce, even the Department of Agriculture. In 1972-1973 the Soviets were able to purchase record amounts of grain because of information they had obtained by eavesdropping on calls to and from the Department of Agriculture. Long-distance calls are transmitted by microwave and are not encoded; it is a simple matter to intercept and listen to messages. Information about grain transactions are not the only communications to travel insecurely; everything from banking information to trade secrets is subject to the same type of attack. Dissemination of research on cryptography may make the NSA's job more difficult. In a society where information is a commodity, there is no easy path between Scylla and Charybdis.

In the two years since the PCSG recommendations and the decision that both NSF and NSA would fund cryptology research, the mathematics community has reached a temporary accommodation with the situation. The AMS has chosen to publicize, without endorsement, any request by the NSA for individuals to participate in the review process. The leading professional organization in computer science, the Association for Computing Machinery, encourages authors of papers in cryptology to submit their articles to the NSA for prepublication review, but does not enquire if that has been done. The NSA has received copies of thirty-five papers, and has suggested "minor changes" in two of them. New funding procedures have not had a sufficient time for evaluation. The NSA has funded four grants, while the NSF has experienced a ten percent increase in cryptology proposals submitted, the same growth it has had in other areas of theoretical computer science. But two years is a short time to measure change in a research community, and it is probably too soon to tell if the NSA restraints will have a chilling effect on research in public sector cryptography.

NSA actions relate directly to basic research in mathematics and computer science. For example, the security of the Rivest, Shamir and Adleman system relies on factoring being hard. Does the NSA propose to suppress investigations on factoring integers? The Atomic Energy Act created a precedent for private work being "born classified," but there is a sharp distinction between ideas which apply to the building of bombs, and those which relate to the security of computer systems. If work on cryptography is restricted in the United States, there is nothing to prevent researchers in other countries from pursuing such inquiries. At the time of hearings on the Atomic Energy Act, Enrico Fermi commented, "Unless research is free and outside of control, the United States will lose its superiority in scientific pursuit." Scientific questions do not arise in a vacuum, nor do ideas develop under the threat of restraint. Restricting the freedom of inquiry in which science thrives is not a decision to be taken lightly.

Bibliography

Adleman, L., Pomerance, C., and Rumely, R., *On distinguishing prime numbers from composite numbers*, Annals of Mathematics, (to appear).

Broad, W., *Evading the Soviet ear at Glen Cove*, Science, 3 September 1982, pages 910-911.

Coppersmith, D., and Winograd, S., *On the asymptotic complexity of matrix multiplication*, Proceedings of the 22nd Annual Symposium on Foundations of Computer Science, October 1981, pages 82-90.

Davida, G., *Safety in numbers*, The Sciences, July/August 1981, pages 9-14.

Diffie, W., and Hellman, M., *New directions in cryptography*, IEEE Transactions on Information Theory, November 1976, pages 644-654.

Inman, B. R., *Cryptography research funding*, Science, 10 October 1980, page 134.

Kolata, G. B., *Cryptography: A new clash between academic freedom and national security*, Science, 29 August 1980, pages 995-996.

Kolata, G. B., *NSA seeks research proposals*, Science, 11 September 1981, page 1233.

Kolata, G. B., *NSA asks to review papers before publication*, Science, 19 March 1982, page 1485.

Lehmer, D. H., *Strong Carmichael numbers*, Journal of the Australian Mathematical Society, Series A, volume 21, June 1976, pages 508-510.

Mathematical and Computer Sciences Advisory Subcommittee, *The role of the NSF in supporting cryptological research*, A Report to the National Science Foundation by its Mathematics and Computer Sciences Advisory Subcommittee, July 13, 1981.

Miller, G. L., *Riemann's hypothesis and tests for primality*, Proceedings of the Seventh Annual ACM Symposium on Theory of Computing, May 1975, pages 234-239.

Public Cryptography Study Group, *Report of the Public Cryptography Study Group*, American Council on Education, February 1981; reprinted in the *Notices of the American Mathematical Society*, October 1981, pages 518 to 526.

Rivest, R. L., Shamir, A., and Adleman, L., *A method for obtaining digital signatures and Public-Key cryptosystems*, Communicatons of the ACM, February 1978, pages 120-126.

Shapley, D., and Kolata, G. B., *Cryptology: Scientists puzzle over threat to open research, publication*, Science, 30 September 1977, pages 1345-1349.

Solovay, R., and Strassen, V., *A fast Monte-Carlo test for primality*, SIAM Journal of Computing, 1977, pages 84-85.

U.S. Congress, House of Representatives, Thirty-fourth Report by the Committee on Government Operations, *The Government classification of private ideas together with additional views*, House Report 96-1540, December 1980.

Walsh, J., *Shunning cryptocensorship*, Science, 12 June 1981, page 1250.

Wilford, J. N., *Science agency blocks funds to aid research on computing coding*, The New York Times, August 27, 1980, page A1.