Business
THE BOSTON GLOBE • THURSDAY, APRIL 6, 1995

A prime argument in patent debate

By Simson Garfinkel
SPECIAL TO THE GLOBE

In a move that will likely inflame the debate over the government's patent application procedures, a California mathematician has received what is believed to be the first patent on a prime number.

But collecting royalties for its use might be difficult.

Actually, Roger Schlafly has patented two prime numbers, but only when they are used together. According to the US Patent and Trade office, the numbers are trademarked under patent No. 5,373,560, a figure that doesn't nearly approach the size of the two patented numbers themselves – one is 150 digits long, the other 300 digits.

The patent, titled "partial modular reduction method," was awarded to Schlafly, an independent mathematician and specialist in the field of cryptography, in December but only recently came to public attention.

The patent claims a new technique for finding certain kinds of prime numbers, which can be used to rapidly perform the kinds of mathematical operations necessary for public key cryptography.

(A prime number is a number that cannot be evenly divided by any number other than 1 and itself. The numbers 2, 3, 13 and 29 are all prime and are not covered by any known patent. Public key cryptography is a technique, based on prime number theory, that allows two individuals to exchange secret messages by computer.)

"I'm sure if you just went to

PRIME, Page 70

Mathematician offer a prime argument in patent debate

■ PRIME

Continued from page 69

someone and said, 'Can you patent a prime number?' they would say 'No, that's ridiculous,'" said Schlafly, interviewed from his home in Soquel, near Santa Cruz, Calif. Schlafly said he developed the patented algorithm while working on a program called SECRET AGENT, which is used to encrypt electronic mail. He added the patent claims for the two prime numbers as an experiment. "I was kind of interested in pushing the system to see how far you could go with allowable claims."

Nevertheless, Schlafly said, the two prime numbers satisfy the Patent Office's conditions for patentability: They are useful, have never been used before by anyone else, and their use for this particular technique is not obvious.

Others see the prime number patent as evidence that the patent office has lost its grip on the patenting process.

"That's outrageous," said Pamela Samuelson, a professor of law at the University of Pittsburgh and an expert on software patents and copyrights.

"It also seems inconsistent with some of the recent decisions issued by the Federal Circuit [Court of Appeals] ... Unless you claim some physical structure [that is used by] an algorithm or a data structure, you can't patent it."

Nearly two years ago, the patent office awarded a sweeping patent that covered the field of multimedia to Compton's New Media. At the time, an outraged computer industry argued that there was nothing new or novel in Compton's programs that deserved a patent. Eventually, the patent office reconsidered the Compton's patent, and threw it out.

Whether or not that will happen with Schlafy's patent remains to be seen. Under most circumstances, patents are invalid if the invention that they described is published before the patent application is filed.

"There are entire journals and conference proceedings devoted to the general subject of this application," says Gregory Aharonian, who published the Internet Patent News Services and maintains a database of several hundred thousand pieces of software art. But few software patents that have been awarded in recent years cite any prior art other than previous patents, Aharonian says.

But whereas the algorithm may be covered under the doctrine of prior art, says Aharonian, the prime numbers themselves are probably patentable. "The claiming of certain prime numbers as part of an encryption process doesn't seem to me to be unnatural," said Aharonian. "I can claim certain specific chemicals as part of a chemical engineering process, so why not a specific number as part of a math engineering process?"

The numbers claimed in the patent are 512 bits and 1,024 bits long, or roughly 150 and 300 decimal digits. While these numbers are quite large by everyday standards, they are typical of the size of numbers used for cryptographic processes. By design, the numbers are so large that it is exceedingly unlikely that a person could guess them or otherwise intentionally discover what they are.

The two principle techniques of public key cryptography were discovered and patented by scientists at Stanford University and at the Massachusetts Institute of Technology in the 1970s. In 1990, they were both licensed to Public Key Partners, a holding company based in California. Last year, Schlafly filed suit against PKP in federal court, claiming that the PKP patents are invalid.

Regarding his own patent, Schlafly said, its real value is the technique that it describes for finding the special prime numbers, rather than the two specific prime numbers that it describes. "I really don't anticipate somebody reading this patent and saying, 'look, here's a good prime number, let's use it!'" he said.

Nevertheless, the patent gives Schlafly the legal right to sue anybody in the United States for using his numbers without permission. "I suppose that you can tell people that if they want to license these prime numbers, they should just call me up."