

# Minesweeper could hold key to Net security

By Gareth Cook, Boston Globe Staff, 11/1/2000

The key to solving one of the most vexing and profound problems of modern mathematics could lie in a most unusual place: Minesweeper, a simple computer game that rivals solitaire as an office time-waster.

The math problem, called the "P versus NP conjecture," asks why some questions are so difficult to answer with computers. It is considered so important that in May the Clay Mathematics Institute in Cambridge offered a \$1 million prize for a solution. Proving the conjecture false would mean that modern encryption technology, the foundation of electronic commerce, would be open to easy attack.

In the spring issue of the journal *Mathematical Intelligencer*, a British specialist in mathematical logic demonstrated that the conjecture would be false if someone can crack Minesweeper, a game in which players race to clear a path through a sea of explosives.

Mathematicians hope the insight, the topic of an open lecture tonight at Harvard University, would bring the public in on a drama that, among specialists, has generated the same fervor that mariners of another age once brought to their search for a passage around the world.

"I have sometimes dreamt that someone found a solution," said Michael Sipser, an MIT math professor who has spent two decades and "about 15,000 hours" searching for the secret. The dreams "filled me with an intense mixture of curiosity and envy," he said.

Engineers are already building processors that run faster than a previous generation could imagine, powering computers that can conquer chess or generate directions from Boston to Walla Walla, Wash., in an instant. But the "P versus NP conjecture," Sipser said, is an attempt to draw, with mathematical certainty, the boundary beyond which computers, no matter how powerful, cannot cross.

"This is enormously fundamental," said Ian Stewart, who is delivering the Harvard lecture and is a columnist for the magazine *Scientific American* and professor at the University of Warwick in England.

Minesweeper, which is included free with the Windows operating system, does not look like the kind of game that would fascinate theorists. The gamer clicks squares of a grid on which mines have been hidden. Numbers then appear, indicating the number of mines in surrounding squares. Using these clues, the aim is to find all the mines.

Intrigued by the kind of logic puzzles the game generates, Richard Kaye of the University of Birmingham in England posed "the minesweeper consistency problem": Given a board of numbers, is it possible to determine whether the clues are consistent with the rules?

This question took him to outer reaches of computer science and to the essence of the "P versus NP conjecture." Many common problems, including multiplying large numbers or putting a list in alphabetical order, are what computer scientists call "P" problems, readily solvable by computer.

On the other hand, "NP" problems seem far more difficult; the only known solution is to break the problem into a large, often prohibitively large, number of P problems. One example is the classic "traveling salesman" question: If a salesman has to visit certain cities, what is the fastest route? Breaking the codes used to protect Internet communications is also an NP problem.

But perhaps, some mathematicians have suggested, the NP problems are actually no more difficult than P problems; they just look that way because nobody has been inventive enough to find an easy way to solve them. Although mathematicians assume this is wrong, they still have not been able to

## LECTURE SERIES

'Minesweeper Math'  
6:30 tonight  
Emerson Hall  
Room 105  
in Harvard Yard  
*Free, open to the public*

prove the resulting "P versus NP conjecture" true after more than two decades of intense labor and several false alarms.

Kaye's contribution, scrawled on loose sheets of paper during his daily train ride to work, was showing that the "minesweeper consistency problem" is "NP complete," that a solution would mean that all NP problems are easily solvable.

So, write a program that can decode Minesweeper for any size board, and you will join the pantheon of mathematical greats, alongside Euler and Pythagoras.

And, of course, there is that million-dollar prize.

The prize offered for the "P versus NP conjecture" is one of seven different million-dollar prizes for what the Clay Mathematics Institute considers to be the most important mathematical challenges of the new millennium, according to Clay president Arthur Jaffe.

In the meantime, word that minesweeper has attained a new veneer of respectability will no doubt be treated with caution by recovered addicts.

"The first night I started playing it, my wife woke up at 3 in the morning and said, 'What are you doing?'" said Rick Kane, an orthopedic surgeon at Noble Hospital in Westfield.

"Now," he said with a tentative laugh, "I'm going to have to start playing again."

*"Minesweeper Math," a free lecture open to the public, takes place at 6:30 this evening in Emerson Hall Room 105 in Harvard Yard.*