Arcane art of encryption sheds light on secrecy

By Peter Woodall, Sacramento Bee

When Matt Franklin told people he was a cryptographer five years ago, they'd ask him if he worked with frozen bodies, or perhaps Egyptian hieroglyphics.

But the explosive growth of the Internet has raised the profile of what was once an obscure profession practiced by mathematicians working for government spymasters.

"Now, it's been in the news enough and people go 'Yeah, hackers and viruses,' " said Franklin, an associate professor of computer science at the University of California, Davis.
At least they're on the right track these days, Franklin said.

The word cryptography comes from the Greek kryptos, "secret," and graphos, "writing."

Cryptography's underlying purpose is figuring out how to defend against enemies such as malicious hackers, also known as crackers. Its practitioners strive to ensure secure communication across an insecure medium, whether that means enemy territory or the Internet.

Encryption algorithms -- sets of mathematical instructions that disguise information -- are used to protect a wide spectrum of electronic communication, from cell phone calls to online credit card and consumer information.

As applications for cryptography have multiplied, so too has research money. Franklin's work was recognized in lucrative fashion last month when the David and Lucille Packard Foundation awarded him a five-year, $625,000 fellowship in science and engineering.
He'll use the money to pursue his research into systems that, he said, "allow mutually suspicious parties to collaborate in ways that are beneficial to all sides."

Keeping information secret using encryption algorithms is just the first step in building these more complex systems. Elections, auctions, purchases and negotiations require more than a secure communication pipeline between two parties.

"The threat isn't only from hackers outside," Franklin said. "The threat is the person on the other end."

Franklin is working on developing electronic voting systems with built-in assurances.

"If you submit your vote, you want to make sure the vote you submit gets there, and that it doesn't get read (along the way)," Franklin said. "But you also care that your vote remains secret and that it is counted."

Recently, Franklin and Dan Boneh of Stanford University developed an improved method for "identity-based" encryption. The Franklin-Boneh system uses a person's e-mail address to encrypt messages rather than requiring that both parties agree on a secret key ahead of time.

Franklin said, looking back, he can spot the childhood inclinations that helped lead to his present occupation.

"I grew up playing a lot of games -- card games, board games," he said. "There's something game-like about cryptography. You're battling some adversary, some opponent."

He first encountered cryptography in a Scientific American article he read in the late 1970s while in high school.

"There was this new revolution then. You could communicate securely with someone you hadn't met. Before this, you had to be given codes ahead of time."

Franklin took his first cryptography class in the mid-1980s at UC Berkeley while working on his master's degree in mathematics.

"I wanted something that would use mathematics," he said. "I thought it was fun, but I wanted to have an application to the real world."

Franklin went on to earn a Ph.D. in computer science from Columbia and spent the next six years doing cryptographic research at Bell Labs in New Jersey and Xerox PARC in Palo Alto.

If Franklin had entered the field two decades earlier, he probably would have worked for the State Department, law enforcement or the military, instead of private industry.

Coded messages have been used in diplomacy and warfare for more than two millennia. Julius Caesar used cryptography to communicate with his troops, and the North used coded flags during the Civil War.

Cryptographers helped the Allies achieve some of their most stunning successes during World War II. They were usually one step ahead of the enemy after British mathematicians cracked the supposedly unbreakable codes produced by the German Enigma machine and American cryptanalysts broke the Japanese code known as Purple.

Criminals and people trying to hide from the prying eyes of oppressive governments also have a long history of using secret messages.

Rum-runners during Prohibition developed complex radio codes to elude U.S. Treasury agents. And American slaves sewed coded quilts in the early and mid-1800s to help guide them as they escaped to the North.

Today, computer encryption programs are widely available and easy to use. Their potential for criminal use worries law enforcement, but the Internet's fluid nature and the efforts of civil libertarians have stymied attempts to regulate distribution.

"The basic information is so widely disseminated at this point, you really can't stop it," Franklin said.

The Sept. 11 terrorist attacks have renewed interest in opening electronic communication to the eyes of the government.

Sen. Judd Gregg, R-New Hampshire, proposed shortly after the attacks that all encryption products have backdoors allowing government surveillance.

Most members of the cryptographic community oppose such plans, Franklin said.

"The consensus is that it shifts the balance too much," he said. "We have to think very carefully about how we respond to this thing, if only because it's not going to prevent terrorists from using something else."

Opponents to Gregg's proposal point out that no evidence that the terrorists encrypted e-mail has been made public. The terrorists would have called attention to themselves if they had done so, Franklin said, because e-mail is rarely encrypted.

"It's as if the whole world is using postcards and you're using a letter," he said.