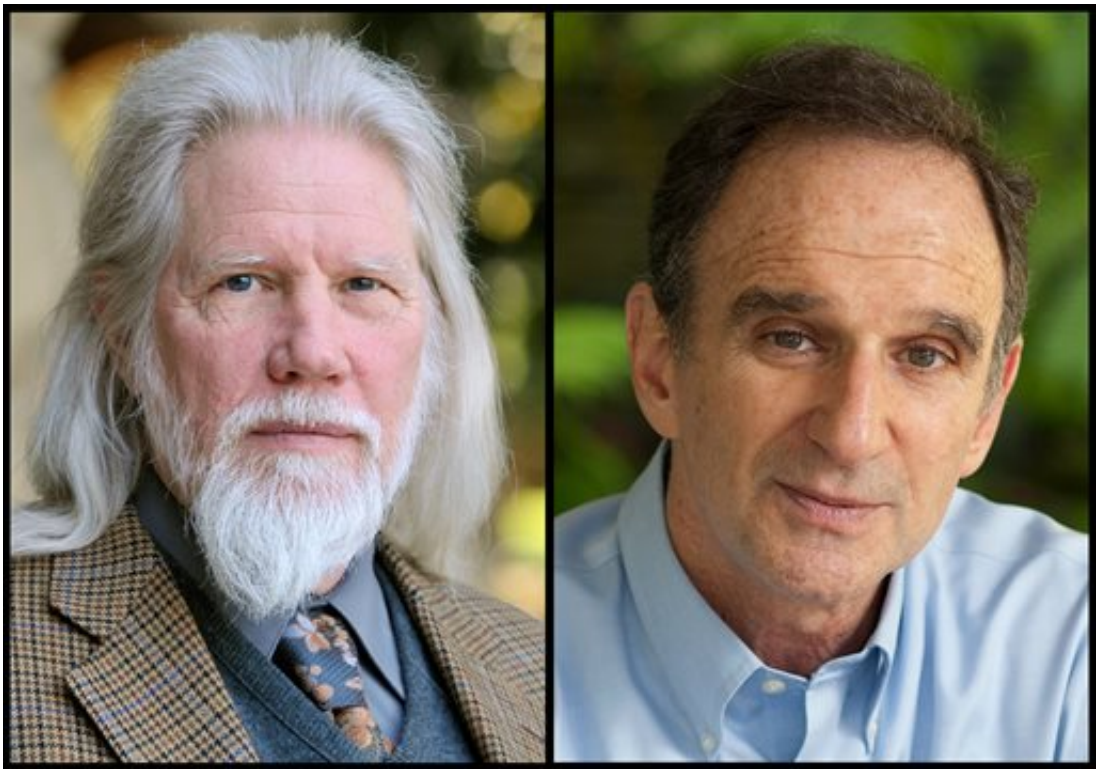
$1M Turing Award winners advocate for encryption

March 1 2016, by Bree Fowler



This photo combination of images provided by Stanford University show Whitfield Diffie, left, and Martin Hellman. Diffie, a former chief security officer of Sun Microsystems, and Hellman, a professor emeritus of electrical engineering at Stanford University, have won the year's $1 million A.M. Turing Award, announced Tuesday, March 1, 2016, by the Association for Computing Machinery. (Rod Searcey, Linda A. Cicero/Courtesy of Stanford University via AP)

This year's $1 million A.M. Turing Award goes to a pair of cryptographers whose ideas helped make the Internet possible. Both men say giving governments control over encrypted communications puts everyone at risk.

Whitfield Diffie, a former chief security officer of Sun Microsystems, and Martin Hellman, a professor emeritus of electrical engineering at Stanford University, introduced the ideas of public-key cryptography and digital signatures back in 1976. The concepts now secure all kinds of data, from online communications and financial transactions to Internet-connected infrastructure like power plants.

The honor was announced Tuesday, the same day that FBI Director James Comey and Apple's top lawyer appealed to Congress for help as the government seeks to force the technology company to hack into a terrorist's iPhone.

Diffie, 71, and Hellman, 70, gained first-hand experience with issues of security and privacy as Stanford researchers in the 1970s.

Before their innovations, electronic communications mainly involved friends talking to friends, and governments tightly controlled encryption technology. The advent of public keys and digital certification enabled the private sector to make it possible for anyone to talk to anyone.

"What we did was reduce the need to know people before talking to them," Diffie told The Associated Press.

Their research did not make them popular with the government. The National Security Agency sought to contain their technology, an effort that became known as the first "crypto war."

Diffie sees the fight with Apple as just one small move in a much bigger

government attempt to grab power.

"I think the people who will control the machines will control the world of the future," Diffie said. "Therefore, everyone today is jockeying for their position with those machines, and this is just one aspect of that."

Hellman told the AP that he sympathizes with efforts to investigate the attack, at least partly inspired by the Islamic State group, in which a couple killed 14 people before dying in a gun battle with police. But he said giving in to the FBI would unleash "huge" consequences.

"The problem isn't so much with this first request, it's the precedent that it would set and the avalanche of requests that would follow," Hellman says, adding that many would likely come from less democratic governments such as China, Russia and Saudi Arabia.

Hellman says he will sign onto one of the many "Friend of the Court" briefs backing Apple in the case. Tech giants such as Google, Microsoft, Facebook and Twitter have pledged to participate as well.

Difffie, for his part, co-authored a paper with other prominent cryptographers last year posing a host of tough questions the U.S. government should answer before it demands "back doors" for law enforcement.

Their award, from the Association for Computing Machinery and mostly funded by Google Inc., is named for British mathematician Alan Turing, and is one of the most prestigious prizes in computing. Past recipients have included Douglas Englebart, who developed the mouse and other computing technologies, and Vint Cerf and Bob Kahn, who developed the key communications protocol behind the Internet.

Hellman said it's nice to be recognized with the award, one of a handful

he's received for his work in encryption over the years. He plans to use his $500,000 share to fund the publication of a book he's writing with his wife of nearly 49 years that looks at what goes into a successful marriage and how those same principles can be applied to creating a more peaceful and sustainable world.

"Holistic solutions are what we need to get past our narrow visions and get to something that works for everyone," he said.