Adi Shamir

Mr. Chancellor, I present Adi Shamir.

Adi Shamir is the Paul and Marlene Borman Professor of Applied Mathematics at the Weizmann Institute of Science in Israel. He is one of the world's preeminent cryptographers and has made several seminal contributions that have helped to shape the field of cryptography.

Professor Shamir is best known for his invention, with Ron Rivest and Len Adleman, of the Rivest-Shamir-Adleman (or RSA) public-key encryption and digital signature schemes in 1977. RSA is the critical technology that provides the security features of many standardized communication systems, including the Secure Sockets Layer protocol used to secure web-based electronic commerce and the Secure / Multipurpose Internet Mail Extensions standard for secure email. For the past twenty years, RSA has been taught in the first-year algebra course in the University of Waterloo's Faculty of Mathematics.

Professor Shamir has contributed many innovative ideas and techniques for analyzing the security of symmetric-key and public-key cryptosystems. Some examples are the first practical attack on the Merkle-Hellman knapsack encryption scheme, the notion of differential cryptanalysis, which has been used to attack block ciphers, practical attacks on the widely-deployed RC4 and A5/1 stream ciphers, and hardware designs for implementing integer factorization algorithms.

He has also contributed fundamental notions and primitives in cryptography, including secret sharing, identity-based cryptography, the Fiat-Shamir identification and signature schemes, and visual cryptography. He has developed methods for broadcast encryption and ring signatures, and protective techniques against side-channel attacks such as power analysis.

For his invention of RSA, Professor Shamir was awarded the Turing Award in 2002 by the Association for Computer Machinery, an award widely considered to be the "Nobel Prize" for computer science. His other accolades include the 1983 Erdös Prize, the 2000 IEEE Koji Kobayashi Computers and Communications Award, and the 2008 Israel Prize.

Mr. Chancellor, in recognition of his outstanding contributions to cryptography, I request that you confer the degree Doctor of Mathematics, *honoris causa*, upon Adi Shamir.