THE ADOLESCENCE OF PUBLIC-KEY CRYPTOGRAPHY

Whitfield Diffie

Northern Telecom, 685A E. Middlefield Road,
94043 Mountain View, CA, USA

Abstract

Public-key cryptosystems separate the capacities for encryption and decryption so that 1) many people can encrypt messages in such a way that only one person can read them, or 2) one person can encrypt messages in such a way that many people can read them. This separation allows important improvements in the management of cryptographic keys and makes it possible to 'sign' a purely digital message.

Public-key cryptography was discovered in the Spring of 1975 and has followed a surprising course. Although diverse systems were proposed early on, the ones that appear both practical and secure today are all very closely related and the search for new and different ones has met with little success. Despite this reliance on a limited mathematical foundation public-key cryptography is revolutionizing communication security by making possible secure communication networks with hundreds of thousands of subscribers.

Equally important is the impact of public-key cryptography on the theoretical side of communication security. It has given cryptographers a systematic means of addressing a broad range of security objectives and pointed the way toward a more theoretical approach that allows the development of cryptographic protocols with proven security characteristics.

J.J. Quisquater and J. Vandewalle (Eds.): Advances in Cryptology - EUROCRYPT '89, LNCS 434, p. 2, 1990.