The Design and Analysis of Cryptographic Protocols

Richard A. DeMillo
Nancy A. Lynch
Michael J. Merritt
School of Information & Computer Science
Georgia Institute of Technology
Atlanta, Georgia 30332
Phone: (404)894-3180

Cryptographic functions are employed by algorithms called cryptographic protocols to provide such services as secret communication, digital signatures and key distribution. New applications are being devised constantly. These protocols are subject to a wide range of attacks, and are often too complex to be easily analyzed. By formalizing the notion of a cryptographic protocol, clear, formally stated security properties for protocols are derived from the simpler security properties of cryptographic functions (proven or assumed). The formalism is applicable to a wide range of communications environments, and is powerful enough to provide non-existence proofs of protocols for particular applications. Introducing non-determinism permits the examination of a useful class or probabilistically secure protocols.

This page was left blank intentionally