Index

Editor's Biography

Gustavus J. Simmons received the Ph.D. degree in mathematics from the University of New Mexico, Albuquerque. He is Senior Fellow for National Security Studies at the Sandia National Laboratories, Albuquerque, NM. Earlier he was Manager of the Applied Mathematics Department and Supervisor of one of two divisions at Sandia devoted to the command and control of nuclear weapons. In all these positions he has been primarily concerned with questions of information integrity arising in national security: command and control of nuclear weapons, verification of compliance with various arms control treaties, individual identity verification at sensitive facilities, etc. His research has been primarily in combinatorics and graph theory and in the applied topics of information theory and cryptography, especially as applied to message authentication and systems design to achieve this function. His current research is aimed at devising information dependent protocols whose function can be trusted even though no specific inputs or participants can be. The need for such protocols arises frequently in questions of national security ranging from simple two-man control schemes for nuclear weapons to arbitrarily complex concurrence schemes for the initiation of various treaty controlled actions. Within the defense community he has pioneered in applying these techniques to the command and control of nuclear weapons.

Dr. Simmons was the recipient of the U.S. Government's E. 0. Lawrence Award in 1986. The accompanying citation reads in part: "In the political climate that has emerged in the nuclear era, increasing importance in the design of nuclear weapons must be placed on control features including verification, authentication, and positive use control. This is the first time that achievements in this field, of vital importance to national security, have been recognized by a Lawrence Award. . . . " In that same year, he also received the Department of Energy Weapons Recognition of Excellence Award for "Contributions to the Command and Control of Nuclear Weapons."

Dr. Simmons was awarded an honorary Doctorate of Technology in May 1991 by the University of Lund (Sweden) in recognition of his contributions to communications science and to the field of information integrity. The diploma cites him as "The Father of Authentication Theory."

Dr. Simmons has published more than 120 papers and books, many of which are devoted to the analysis and application of asymmetric encryption techniques or to message authentication, and has been granted several patents for inventions in this area. At the invitation of the editors, he wrote the section on cryptology that appears in the 16th edition of the Encyclopaedia Britannica. He is an editor for Journal of Cryptology, *Ars Combinatoria*, and *Codes, Designs and Cryptography.*