J. Cryptology (1988) 1: 1

Journal of Cryptology

Editorial

Although the study of cryptology is of great antiquity, there was very little public research before the mid 1970s and, consequently, no need for a research journal devoted to this subject. The past decade, however, has witnessed an explosion in research in both cryptography and cryptanalysis. Much of this research has appeared in conference proceedings and has not found its way into refereed journals, or else has been published in journals for whose primary audience the subject was of secondary interest. The result has been a wide dispersal in the literature of fundamental new results. This situation prompted the International Association for Cryptologic Research to initiate a new journal dedicated to research in cryptology.

The main goal of the *Journal of Cryptology* is to provide a forum for the publication of important new results and surveys in all areas of cryptography and cryptanalysis. A broad spectrum of research will be covered, from theoretical results to application issues.

A new journal can only be successful as the result of the combined efforts of a large number of dedicated individuals. Noteworthy among these are the members of the editorial board and the board of directors and the officers of the IACR. Many of the referees have put forth a commendable effort to assist the authors in improving their manuscripts. We would like to express our sincere gratitude to all of them. We would especially like to thank the authors who have submitted their work to the new journal, for they have provided the motivation for the efforts of all the rest of us. We would also take this opportunity to solicit more submissions; we hope that this first issue will encourage potential authors. We welcome any comments or suggestions that you have.

Ernest F. Brickell