Preface

This issue contains a collection of papers on five subjects: the use of computer technology for multimedia presentations, case studies in enterprise modeling, efficient implementation of cryptographic systems based on exponentiation, extensions to the semantic model for relational databases, and a case study in real-time software portability. In addition, there is a special contribution by the associate editors—a guide for authors who wish to submit papers to the *Journal*. A list of currently available *Journal* paper reprints is included as well.

The first paper, by Moore, describes tools and techniques that are available on the IBM Personal System/2® to develop and replay multimedia presentations. The key components of this multimedia capability are the Audio Visual Connection® (AVC™), the Musical Instrument Digital Interface (MIDI), the Audio Capture and Playback Adapter, and the Video Capture Adapter. These supporting hardware adapters and software products are designed for fully digitized audio and video. The resulting creations can span the range from passive informational presentations to fully interactive applications supported by databases. The cover for this issue was developed in part using the capabilities described in this paper.

In a recent series of studies, nine IBM customers utilized the modeling features of the Information System Model and Architecture Generator (ISMOD) to explore their present and future needs for enterprise and information support through computers. The author, Katz, was directly involved in these studies and reports on their impact on creating tactical and strategic plans for existing computer systems, on computer availability under disaster conditions, and on planning for distributed computer support in an overburdened, single-host environment. This work builds on 10 years of studies involving over 450 IBM customers in need of business and enterprise modeling capabilities. The results are both qualitative and quantitative, including a sophisticated understanding of how such extensive and important studies support business needs and provide cost savings.

Much attention has focussed in recent years on the ability to encrypt intercomputer transmissions for security and authentication purposes. One of the most sophisticated current encryption styles is exponentiation, which is used to provide public key algorithms for encoding and decoding messages and is the basis for bulk encryption in the Data Encryption Algorithm. A major concern in using such algorithms on personal computers is their execution time. Comba shows how the execution speed of exponentiation algorithms can be made effective for the IBM Personal Computer (PC).

Hirao describes recent work to extend the relational database semantic model so that it provides formal specification of data definition for information representation, constraints for information integrity, and valid operations on the information. These three parts—structural, integrity, and manipulative—are explored through new data models such as the Non-First-Normal-Form model (NF2) and the deductive database model. New database systems built using these principles would allow for manipulation of incomplete and ambiguous information, make use of facts and rules, and maintain data integrity.

The conversion of software from one hardware base to another is both important to industry and fundamentally difficult. Britcher shows how this work was performed by IBM and two other companies for a part of the Federal Aviation Administration's New York terminal approach control facility. This work was complicated by the changes in machines, operating environments, and programming languages, and because the system is a real-time application. Formal methods and recording played a large role in the success of the project. The overall effect was conversion of the working system at less cost and

with less loss of evolutionary (and sometimes undocumented) capability than could be expected from starting anew.

We have included a revised and updated edition of our guide for authors of the *Systems Journal*. Anyone who wishes to submit a paper for publication in the *Journal* should read this guide. Its basic functions are to ensure that submissions are appropriate for the *Journal* and to save both the author and the editorial staff unnecessary rework. Making use of this guide and perusing a few recent issues should ease the publication process for all who are involved.

Since 1975 the *Journal* has made reprints of individual papers available to our readers. At the end of this issue is a list of all reprints that are currently available. Ordering instructions are given with the list.

The next issue of the *Journal* will have sets of papers on two themes: the recently announced VM/ESA operating system and advances in cryptographic systems.

Gene F. Hoffnagle
Editor