Foreword

Having spent most of my adult life working with the design, development, production, and deployment of secure communications equipment and networks used by over 90 countries and many multinationals, it is an honor and pleasure to write this foreword.

It is quite striking that as I draft this piece, TJX Companies, Inc. revealed some 45.6 million credit and debit card numbers were stolen from two of its systems over the better part of two years. This happening in fact is just one in a long series of information compromises—albeit a big one—that could have been mitigated via the application of cryptographic tools, policies, and procedures.

Because we live in a world today where we basically have a ONE to ALL relationship via the interconnectivity of the Internet, the two fundamentals of good security—BORDERS AND TRUST—take on new meaning. This new dynamic in security requires the application of cryptographic tools and practices regarding information, and the access, use, storage, transmission, and destruction of that information over its life cycle. In fact this problem will only grow as: (1) assets move from the physical to the virtual realm (bits and bytes), (2) information grows at a rate of 2+ exabytes a year—a "target rich" environment, and (3) more and more of the world's population becomes "connected."

As most professionals know, comprehensive, understandable, and easy to read treatises on complex, mathematically based subject matter are usually few and far between. So too with cryptography. However, with this volume professor Mogollon not only addresses the historical foundations of cryptographic tools and methods, but delivers a very clear and understandable picture of the breadth and depth of secure communications today. And he does this while providing very clear graphics on how historical and modern approaches and systems work. The clarity of these examples and the understanding they impart is unparalleled in technical literature.

This book is a must read for all professionals as the application of the tools and methods discussed herein are a required "best practice" today. And it will serve as a useful reference for years to come.

Dr. John H. Nugent, CPA, CFE, CISM, FCPA

Director of the Center of Information Assurance, University of Dallas