Foreword

In February 2004, at the Universitat Politècnica de Catalunya, we presented a 45-hour *Advanced Course on Contemporary Cryptology*, organised by the Centre de Recerca Matemàtica. This volume is an expanded and unified version of the material presented in the lectures and the background material that we distributed among the participants.

As the title implies, our aim in the course and in this text is to treat selected topics of the subject of contemporary cryptology, structured in five quite independent but related themes: Efficient distributed computation modulo a shared secret, multiparty computation, modern cryptography, provable security for public key schemes, and efficient and secure public-key cryptosystems. The beauty and multidisciplinarity of this topic motivated the interest of the participants, to whom we are very much indebted for their helpful contributions.

Thanks are due to the Centre de Recerca Matemàtica for organising and sponsoring the Advanced Course, to the CRM administrative staff for smoothly working out innumerable details, and to Paz Morillo for the mathematical organisation of the course and for making it such a pleasant experience. Special thanks go to all the participants of the course for their interest in the event and for their many comments on the material.