Preface

The notion of Boolean function was introduced in the second half of the 19th century in connection with investigations in mathematical logic and foundations of mathematics. Boolean functions are named after George Boole (1815–1864), an English mathematician, one of the founders of mathematical logic. In the first half of the 20th century Boolean functions attain fundamental importance in the foundations of mathematics. However, for a long time Boolean functions have not been used in applications.

This situation changed drastically in the middle of the 20th century, when the intensive development of communication technology, instrument-building, and computer technology required the creation of an adequate mathematical apparatus. In this period, applied parts of mathematics such as the theory of finite functional systems, information theory, coding theory, and finally mathematical cryptography have been developed. The practice showed the fruitfulness of the application of Boolean functions to the problems of analysis and synthesis of discrete devices for processing and transformation of information.

The concept of cryptography that has been established in the scientific literature includes a range of scientific areas, each of them having its own subject of investigations and using specific mathematical techniques. Some researchers do abstract investigations "with cryptographic motifs" in the area of computational complexity theory; others are busy constructing and analyzing algorithms for particular cryptographic systems. In many cryptographic areas, Boolean function techniques are often used while formulating and solving various problems. This applies mainly to traditional cryptographic systems with a secret key. The title of the book "Boolean functions in coding theory and cryptography" reflects the relation between many cryptographic problems and encoding and decoding problems for Reed–Muller codes.

In this book, for the first time in Russian, we present cryptographic aspects using Boolean functions techniques. The only exceptions are questions related to complexity theory and solving systems of Boolean functions. In this book both classical and recent results are presented.

To understand the material, university courses of linear algebra, group theory, finite fields theory and polynomials, combinatorics and discrete mathematics will suffice. A knowledge of basics of probability theory is also assumed.

The book is based on courses given by the authors in MGU for students of Mechanics–Mathematics and Computational Mathematics and Cybernetics Departments who major in "Information security". Recent results obtained by the authors in the framework of the scheduled work of the MGU Laboratory on Mathematical Problems of Cryptography are also included in the book.

The book consists of nine chapters.

Chapter 1 is preliminary. It contains basic notions and results of algebra used in the book. In Chapter 2, basic notions and theorems of Boolean function theory are proved. In Chapter 3, problems of Boolean function classification under different groups of transformations are considered. Chapter 4 presents basics of coding theory. In Chapter 5, properties of Boolean functions are considered from the point of view of coding theory. In Chapter 6, properties of maximum-nonlinear functions are studied. Chapter 7 investigates the correlation immunity property of a function. In Chapter 8, various cryptographic characteristics of Boolean functions and mappings are considered in detail. Chapter 9 contains elements of cryptanalysis.

To avoid making the book too large, some of the results are presented as problems. Some of the problems included in the book are still open; they may be a basis for future research.

All items in the text are numbered consecutively within chapters: definitions, theorems, examples, etc. Thus, for example, Definition 1.121 refers to item 121 in Chapter 1 (which turns out to be a definition). The mathematical expressions and figures have similar but independent numbering.

The authors will accept with gratitude any comments on the book. They could be sent to the internet site `http://www.cryptography.ru`.

The authors express their gratitude to Mikhail Vladimirovich Stepanov for his support during the work on the book.