

Preface

For centuries, cryptography, as the science of ciphering or covering information from unauthorised use, had been employed mainly for protecting messages communicated between the military or governmental officials. Therefore, the circle of people employing cryptography was quite restricted and the very methods of this science secret. However, in the last decades, when the mankind has entered the information society stage, cryptographic methods of information protection become widely used, serving, in the first place, business needs. At that, not only inter-bank payments carried out over computer networks are meant or, say, electronic exchanges operating via the Internet, but also numerous transactions in which millions of “ordinary” people are involved every day, such as payments by credit cards, transferring wages onto bank accounts, ordering tickets and buying goods over the Internet, *etc.* It is a natural demand that all these transactions, as well as mobile phone conversations and electronic mail, be secured against dishonest or just overly inquisitive persons and organisations. Therefore nowadays many specialists working in the field of information technologies (IT) are engaged in designing and exploiting the systems of information protection. Since many of the methods used thereon are based on the results of contemporary cryptography, this subject is now studied in the universities preparing IT specialists.

The present book is to a great extent based on the courses taught by the authors at several universities in Russia, Germany, and Finland. The book describes the main techniques and facilities of contemporary cryptography. The topics covered include block ciphers, stream ciphers, public key encryption, digital signatures, cryptographic protocols, elliptic curve cryptography, theoretical security, and random numbers. The preference is given to the methods that become (part of) cryptographic standards.

As the book title suggests, the content of the book is intended to IT students and graduates. The aim of the authors was to provide a comprehensive introductory course of cryptography without resorting to complex mathematical constructions. All themes, even the elliptic curves and theoretical security, are conveyed so that only require the knowledge of secondary school mathematics. Some special facts of number and probability theories are considered when necessary, usually through examples rather than by giving strict and complex proofs. On the other hand, all cryptography results are proved. Thus the intended audience is very wide stretching from the IT specialists who wish to become qualified users of cryptographic algorithms to those who are looking for an elementary course to start a career of the developer of cryptosystems.

In conveying the matter, we tried to follow A. Einstein's principle: "everything should be made as simple as possible, but not simpler". All methods are described in sufficient details to enable their computer implementation. Justification for every method is always given, sometimes with reference to known results in number theory and other fields. When it is appropriate, algorithms written in pseudo-code are provided. All methods are supplied by numerical examples. In fact, for the sake of simplicity, all public-key algorithms are studied in the "integers modulo n " system. The higher algebraic terminology (rings, fields, *etc.*) is not used since it may be foreign to the majority of the intended readers. Nevertheless, all mathematical results (even in case of elliptic curves) are strict and consistent.

The contents of the first 5 chapters can be used as a basis for one-semester course. The other chapters can be read as specialisation courses. Our experience shows that successful learning is facilitated by practising exercises and problems and working in computer laboratories for implementing basic algorithms and systems. Therefore the book contains training problems supplied by the answers and themes for labs.

We hope that the present book will help the reader not only understand the main problems and methods of contemporary cryptography but also estimate the beauty and elegance of its ideas and results.

B. Ryabko

A. Fionov