**ZMATH 2011a.00587**

**Stanoyevitch, Alexander**

**Introduction to cryptography with mathematical foundations and computer implementations.**

Discrete Mathematics and Its Applications. Boca Raton, FL: CRC Press (ISBN 978-1-4398-1763-6/hbk). xix, 649 p. (2011).

The book under review is focused on the main concepts of cryptography. Each chapter contains definitions and theorems, examples of key points. Figures and tables help understand more difficult concepts. The end of each chapter contains exercises, detailed solutions of harder exercises and codes for computer implementations. The book contains twelve chapters and five appendices. The first chapter "An Overview of the Subject" explains the basic concepts of cryptography including an overview of the math that stand beside them. For an starting point the Vigenere and Playfair cipher are exemplified in detail. In the second chapter "Divisibility and Modular Arithmetic" the concepts of divisibility and primes are described and we are introduced to systems of modular integers and their associated arithmetic. The division algorithm and the Euclidean algorithm are explained with definitions and examples. In the third chapter "The Evolution of Codemaking until the Computer Era" provides us with a brief history of the evolution of codemaking from antiquity through the completion of the World War II. The codes are explained using the concepts of functions and modular arithmetic that were described in the first and second chapter. This chapter presents a general and formal definition of a cryptosystem, which will be the pattern that will serve to describe all the cryptosystems that have been developed over time as well as systems that will be devised in the future. We also have the affine cipher, a slightly more general class of ciphers than the shift ciphers, that were presented in the second chapter, that is also easily described in terms of modular arithmetic is the class of affine ciphers. The concept of steganography is described, the technique in which the form of the plain text is left intact, but efforts are made to conceal its existence from unintended recipients. One of the first encryption/decryption machines that was to foreshadow many of the computer-based cryptosystems that would follow in the latter portion of the $20^{th}$ century is the Enigma machine, described in this chapter. Chapter four "Matrices and the Hill Cryptosystem" talks about a very important data structure, the matrix. Mathematical examples, definitions and exercises of matrix addition, subtraction, and scalar multiplication are shown. The Hill cryptosystem is shown, which has an important historical significance since it marked the beginning of a revolution in cryptography in which cryptosystems were reliant on mathematical sophistication. In this chapter the Hill cryptosystem is exemplified and exercises are at hand. "The Evolution of Codebreaking until the Computer Era" is the title of chapter five. In the present chapter we can find details of more sophisticated attacks on computer security are. It begins with an example of how a frequency analysis can be used in a ciphertext-only attack on a substitution cipher. The techniques used here illustrate that, apart from the statistical information, several linguistic techniques are often employed in such attacks. Ciphertext-only attack on the Vigenere cipher that was discovered by Kasiski and Babbage is exemplified followed by a mathematically elegant attack that was discovered by Friedman. Finally, in this chapter historical there are details relating to the famous attack on the Enigma machine that was initiated by Polish codebreakers. In the sixth chapter "Representation and Arithmetic of Integers in Different Bases" we have examples of representations of integers in different bases, hex(adecimal) and binary expansion, conversions between English plaintexts and strings of digits, fast modular exponentiation. Chapter seven "Block Cryptosystems and the Data Encryption Standard (DES)" presents the DES algorithm, the national standard for a secure cryptosystem. More exactly this chapter discusses the rise and fall of DES, and provides a complete description of its functionality. After some related history, next its discussed some preliminary concepts of the more general block cryptosystem on which DES is based. After, a description of a scaled-down version of DES will be exemplified, which will make our subsequent description of the real DES. After describing DES, we can see some interesting technological breakthroughs spurred by efforts to crack DES, along with how DES eventually was broken. The chapter ends with descriptions of some developments of various modes of operation for general block ciphers. Chapter eight "Some Number Theory and Algorithms" begins with the subject of number theory. The prime number theorem, followed by Fermat's little theorem which is presented with an example. The Fermat's little theorem will be generalize using the Euler Phi function to work for any modulus $m$. Euler generalized Fermat's little theorem to work for any modulus. Primitive roots, and other number theory algorithms are exemplified. Chapter nine "Public Key Cryptography", contains an informal analogy for a public key cryptosystem, explaining the advantages that asymmetric key cryptography brings. Further on in the chapter we are introduced with a problem that kept the early innovators Diffie and Hellman captivated, the problem of developing a feasible implementation of a secure electronic key exchange. One-way functions lie at the core of any symmetric key system, it is given out publicly so that anyone can use it, but it would be an intractable problem for anyone to compute the inverse function, this is needed for explaining the Diffie-Hellman key exchange system. System which generations of cryptographers

had been convinced that such a system could not possibly exist due to his striking elegance and simplicity. The security of the Diffie-Hellman key exchange, as well as that of the ElGamal cryptosystem will be introduced later in this chapter, both rely on the difficulty of computing discrete logarithms. The discrete logarithms topic was discussed in the previous chapter, it will be reviewed in this chapter in a slightly less general sense. Next the quest for a complete public key cryptosystem is detailed, resulting the first publicly announced complete and secure public key cryptosystem named RSA. Digital signatures and authentication its a very important concept in the cryptography domain, it is discussed am explained very well in this chapter with examples and exercises that help readers understand the core nature of digital signatures. To bring a more elaborate example of a digital signature the ElGamal cryptosystem is discussed, which is a bit more complicated that the RSA system. Unlike the RSA system, ElGamal has natural extensions to more sophisticated cryptosystems like elliptic curve cryptosystems. The ElGamal system can be used with the general digital signature algorithm to digitally sign documents, but, in this chapter, there is an improved digital signature algorithm for the ElGamal setting. This algorithm allows the possibility of several different legitimate signatures per document, per individual. The Merkel-Hellman knapsack cryptosystem is another public key cryptosystem introduced by Ralph Merkel and Martin Hellman. Such systems are known as knapsack cryptosystems, and their security rests on the difficulty of corresponding knapsack problems. In this chapter the attention is restricted to a single prototypical knapsack problem and its associated cryptosystem. This knapsack cryptosystem is the original one in the Merkle-Hellman paper, the cryptosystem is based on the idea that the secret decryption key will cover an intractable general knapsack problem into one with superincreasing object weights that can be easily solved, the essential aspect of the cryptosystem is an appropriate one-way function. The chapter ends with a discussion about government controls on cryptography, laying out some issues about the restrictions made by governments on what sorts of cryptographic technologies can be sold or given. In chapter ten "Finite Fields in General, and GF($2^8$) in Particular" its talked about the mathematical knowledge needed to understand the next chapters. Binary operations, rings, fields, operations with polynomials ended by the 16-element finite fields GF($2^4$) and 256-element finite field GF($2^8$), these fields will have a crucial role in the scaled-down AES and the full AES cryptosystems of the next chapter. The construction and understanding of these two fields is the main purpose of this chapter. Chapter eleven "The Advanced Encryption Standard (AES) Protocol" begins with describing some of the history and basic facts about the AES cryptosystem. A scaled-down version of AES is presented first, it exhibits almost all of the salient features of the AES. The examples will be made using 128-bit keylength. After the encryption was made the decryption in the scaled-down version of AES is explained. Finally we focus on the AES encryption algorithm and the AES decryption algorithm with a short discussion of its security and reliability. Chapter twelve "Elliptic Curve Cryptography". This chapter focuses on the most important and powerful public key cryptosystem. An cryptosystem based on elliptic curves tends to be 10 time more secure than all other known public key cryptosystems. This has important ramifications for efficient hardware implementations. One of the reasons for this security is the fact that, unlike modular integers, there is no notion for "size" of points in modular elliptic curves. The chapter begins by introducing elliptic curves over the real numbers and rigorously defining their addition operation by means of their graphs. Modular elliptic curves over $\mathbb{Z}_p$ will be discussed further on and introduce the discrete logarithm problem for elliptic curves. This leads to the development of the natural extensions of the Diffie-Hellman key exchange. We can also represent plaintexts using modular elliptic curves. The original ElGamal cryptosystem is reviewed and then the corresponding modifications are illustrated to set up the modular elliptic curves form. The chapter is ended with an example of an elliptic curve-based factorization algorithm. The book ends with four appendices in which we can find answers and solutions to all the exercises in the book and the fifth appendix in which we have suggestions for other books which represent different domains of interest. *Nicolae Constantinescu (Craiova)*

*Classification:* F65 H75 R25
*Keywords:* cryptography; number theory; elliptic curve cryptography