Review of the book

"Decrypted Secrets - Methods and Maxims of Cryptology"

by F.L. Bauer

Springer, 2007

ISBN: 978-3-540-60418-1

Denise Reinert

2009-11-15

1 What the book is about

As the subtitle reveals, the book *Decrypted Secret* discusses different methods and maxims of cryptology. The book consists of two parts: cryptology and cryptanalysis.

The first part of the book gives an overview of cryptology as such and introduces different encryption systems including their structure and method as well as their historical background. As an introduction, the author presents some people from different areas, who played a role in cryptography.

In Chapter 1 (Introductory Synopsis), the author introduces cryptography and steganography by classifying steganographic and cryptologic methods schematically and explaining them descriptively based on historical examples.

Chapter 2 (Aims and Methods of Cryptography) gives a short overview of cryptology as such. After a short historical part which describes the basic aims of cryptology, in the following sections all necessary fundamentals of cryptography (such as plaintext, encryption, decryption, ciphering, coding, character sets and keys) are explained and mathematically defined.

Chapter 3 (Encryption Steps: Simple Substitution) introduces encryptions systems that are based on substitution. Thus, the author goes into the details of unipartite and multipartite substitutions and explains the special case of permutation. Each of the encryption systems is described mathematically and additionally shown using a historic cipher as a concrete example.

Chapter 4 (Encryption Steps: Polygraphic Substitution and Coding) extends the preceding chapter by polygraphic ciphers, introducing bigraphic and trigraphic substitution and tomographic methods. As in the preceding chapter, there is a theoretical description of each method as well as a detailed explanation of the single steps of calculation using a concrete cipher as an example. These examples are supplemented by some historical information, allowing the reader to comprehend the circumstances of the development and the application of the encryption system.

The following chapter 5 (Encryption Steps: Linear Substitition) first introduces the basic concepts of linear (affine) substitution as a special case of polygraphic substitution and then considers different cases in detail (such as self-reciprocal, homogeneous and inhomogeneous, binary and decomposed linear substitution).

In chapter 6 (Encryption Steps: Transposition) encryptions systems that are based on transposition are introduced. The author first explains the basic principles of transposition, then these principles are shown in detail by some easy ciphers and extended in the following sections. Additionally, in the last

section the author discusses the concept as anagrams and their meaning in the course of history.

While the first chapters only dealt with monoalphabetic ciphers, chapter 7 (Polyalphabetic Encryption: Families of Alphabets) introduces polyalphabetic encryption. As before, the basic principles are explained first, then extended by iterated, shifted and rotated alphabets and at least shown in detail by concrete examples. Additionally, some well-known ciphers as Vigenère, Beaufort and examples of unrelated alphabets (Porta, Bazeries) are presented including their historical background. The chapter is supplemented by a section about rotor crypto machines, containing a detailed explanation of the principles of mechanical crypto solutions such as the enigma.

Chapter 8 (Polyalphabetic Encryption: Keys) deals with the generation and the management of keys for polyalphabetic encryption systems. In dependence on chapter 7, there is a section about mechanical solutions, containing also some facts on the enigma. Another section is dedicated to the one-time-pad.

In chapter 9 (Composition of Classes of Methods), some advantages and risks of the composition of encryption systems (or methods) are considered. At the beginning of the chapter, the necessary mathematical basics (group properties) are explained. After several examples for possible compositions of methods and the possible problems, which are going along with these operations, the author presents the encryption systems DES and IDEA.

After the symmetric encryption systems, Chapter 10 (Open Encryption Key Systems) now introduces asymmetric methods for encryption and signature. The author shortly describes the mathematical problems, on which the current asymmetric ciphers are based on. Additionally, there is a section about efficiency of calculation. As a concrete example, RSA is introduced along with some of the popular attacks on RSA.

Chapter 11 (Encryption Security) concludes the first part of the book (cryptography) and leads over to the second part (cryptanalysis). The author discusses some errors, which can occur during the encryption of messages or the handling of encryption systems by a vivid description of historical events. In addition, the author gives advice for the handling of cryptography and its components. The last section discusses the conflict between the state and its citizens concerning the use of cryptography.

After the first part of the book, the author attached some pictures of machines for encryption of different ages, from ancient Greece up to supercomputers.

The second part of the book deals with cryptanalysis and starts with an introducing text about the aims, proceedings and the history of cryptanalysis, which means breaking cryptographic methods or at least encryption systems.

Chapter 12 (Exhausting Combinatorial Complexity) presents the easiest method of cryptanalysis: the exhaustive search (or brute force). The author shows the complexity of the encryption systems, which were described in the chapters before. Additionally, there is some practical advice for performing cryptanalysis by exhaustion and for its mechanizing.

In chapter 13 (Anatomy of Language: Patters) some approaches to the finding of patterns are introduced. The chapter discusses patterns within single words as well as patterns within whole messages, again with a reference to historical incidents.

Chapter 14 (Polyalphabetic Case: Probable Words) extends the simple search for patterns from the preceding chapter to the case of polyalphabetic ciphers. The concept of non-coincidence exhaustion of probable word positions is explained and completed by additional methods like those from de Viaris and Friedman and the method of isomorphs.
Chapter 15 (Anatomy of Languages: Frequency) discusses different methods of frequency analysis. The author explains the occurrence of letters and groups of letters in different languages as well as combined methods. Additionally, the chapter contains a multitude of statistics for the analysis of encrypted messages.

In Chapter 16 (Kappa and Chi), the methods for the analysis of symmetric ciphers are extended by relative frequencies as the index of coincidence (Kappa), and the coefficients Chie and Psi for the detection of the language of a text by analyzing the ciphertext.

In Chapter 17 (Periodicity Examination), the methods from the preceding chapter (Kappa, Chi and Psi) are applied to polyalphabetic ciphers, in order to get some estimations on the length of the period. After a section about cryptanalysis by machines, this chapter also introduces the Kasisky examination.

Chapter 18 (Alignment of Accompanying Alphabets) deals with the problem of reducing the different alphabets of a polyalphabetic ciphertext to only one primary alphabet, if the length of the period is already known. To achieve this, the author applies the methods for frequency analysis, which were introduced in the chapters before, to concrete examples. Additionally, he discusses methods for the reconstruction of keys.

In Chapter 19 (Compromises), one of the errors from chapter 11 is recapitulated and the variety of possible methods of attacks, which can derive from the compromise of a cipher, are described. Among these methods some varieties for the superimposition of plaintexts as well as indicator doubling and the construction of feedback cycles are explained in detail.

Chapter 20 (Linear Basic Analysis) contains a short description of the analysis of linear polygraphic ciphers, such as by the reconstruction of the key and of a linear feedback register.

Chapter 21 (Anagramming) gives a short overview on the analysis of ciphers based on transposition.

In Chapter 22 (Concluding Remarks) the author shows succeeded attacks on encryption systems and ciphers in the historical context and describes the mode of operation of cryptanalysists. Additionally, the meaning of cryptography an cryptanalysis in history is discussed.

The appendix contains an overview of axiomatic information theory.

2 What is this book about?

The book consists of two parts: cryptography and cryptanalysis. In the first part, the author describes a multitude of cryptographic methods and encryption systems with their mathematical background and mode of operation and describes them in detail by using concrete examples.
The second part of the book is about cryptanalysis, which means the breaking of cryptographic methods, which is also described in detail. Additionally, the book contains an extensive history of cryptography, the people who are related with it and their role in military and private situations.

3 What is the book like?

The style of the book is as precise as to be expected from the author Dr. rer. nat. Dr. ès sc. h.c. Dr.rer.nat. h.c. mult. Friedrich Bauer, professor emeritus of mathematics and informatics, Technical University of Munich. The encryption methods are described correctly and without errors, all statements are referenced by literature, so this book is excellent for research purposes and for students.

Characteristic for the book is the continuous proceeding of the author to initially describe the cryptographic systems or the attacs, then to describe them mathematically and finally to show them on a concrete example, which is carried out step by step. Thus the reader can comprehend the learned theory applied on an example. By this approach, the reader additionally gets to know a multitude of historic cipher systems, which eases the comprehension and loosens up the reading (or learning). The author

also introduces most of the current asymmetric encryption systems and even if only a small part of the book is dedicated to these methods, the book contains the important information on their methods of operation and their weaknesses.

Surprising and unaccustomed for such a mathematical book on cryptography and cryptology is the historical background, which is a major thread throughout the book. Thus, the reader does not only learn about the methods of operation and the weaknesses of encryption systems, but also gets to know the social and political backgrounds and the origins of the development of ciphers, attacks against them and the people who were involved in it.

4 Would you recommend this book?

This book can be recommended to everyone who has mathematical, informatical, historical or linguistic interests in cryptography.

There are different ways of approaching this book. Due to its vivid style, it can be read linear as a novel, but it can also be used as reference work for specific topics.
To be able to use the book in its whole scope, some fundamentals in discrete mathematics are advisable, otherwise it would be difficult to fully comprehend the single encryption systems and their attacks.
However, it is not obligatory to read the book thoroughly, a reader with historic interests could browse the mathematical definitions, whereas a mathematician could quickly scan through the details of the incidents of World War II.

As a conclusion, it can be said, that this book is a piece of fascinating literature, which can scarce be found in this combination of contents.

The reviewer is a Ph.D. student at the Institute for E-Business Security (ISEB), Ruhr-University of Bochum.