Review of the book

"Codes and Ciphers"

by Robert Churchhouse

Cambridge University Press, 2002

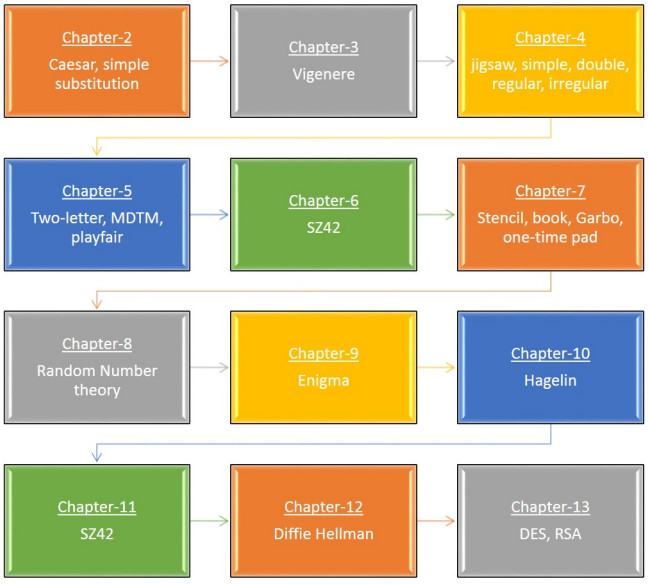
ISBN: 978-0-521-00890-7

Nishant Doshi
MEFGI, Gauridad Campus, India

1 Summary of the review

This book is full of cipher and its examples which is very good for the students and beginners. For researchers this is helpful to understand the inner working of ciphers and to do further research in various cryptographic ciphers. In general, the authors write all the references at once (alphabetic/year-wise) at the end of book, makes hard to find some relevant references. However, in this I surely appreciate the author for taking extra care by writing the references chapter wise. Also, I like the writing of the chapters in series like Ch.2 for substitution cipher with end note as motivation for next chapter. And follow same pattern in several chapters. It would be helpful if after each chapter, the author put/mention some tools that helps to compute or cryptanalysis the ciphers.

For the researchers, this book gives the fundamentals understanding of the ciphers and its cryptanalysis. I recommend this book to the UG students to strengthen their fundamentals on ciphers. For the PG student (and researchers too) to get the well depth understanding with further scope of improvements in the ciphers and its analysis. For simplicity, below figure depicts the list of ciphers (chapter-wise) that were discussed and analyzed in this book.



2 Summary of the book

Chapter 1 In any book, introduction need to introduction of all chapters in concise way and also explains the notations/terminology that were used throughput the book. Indeed, this book is

one of example of this methodology. Each of the subsection start with formal introduction of various topics that were explain in detail in subsequent chapters. On an average, this chapter is an introduction and explains required concepts (including maths) nicely.

Chapter 2 This chapter begins by outlining the Caesar cipher (the cipher to be way old and successful at that time). In security, the historical ciphers like Caesar are at the pioneer and works at base for the today's various known cipher. Thus, to not only study the working of cipher, but to do the cryptanalysis of it is very admiring way that considered by the author. This chapter explains the monoalphabetic simple substitutions cipher with its cryptanalysis.

Chapter 3 After havind sound basis on the monoalphabetic cipher, which is less secure, this chapter deals with advance technique called polyalphabetic cipher. It start by giving overview of vigenere cipher with nice example and cryptanalysis of it. The paragraph entitled "How much text do..." is eye catching and helpful for study of vigenere cipher. At last, the device called jefferson's cylinder is discussed.

Chapter 4 The ciphers that discussed in previous chapters are based on the substitution technique in which each letter of plaintext is replaced by other letter. This chapter discussed about the transposition technique in which each plaintext letter is replaced by another plaintext letter , thus the frequency of letters in plaintext and ciphertext are same. This type of ciphers are more vulnerable to frequency analysis attacks as to other techniques. This chapter discusses the two variation called single and double (more secure) version of transposition cipher. Afterwards, it discusses about regular and irregular techniques for the transposition.

Chapter 5 While the previous chapters deals with monograph technique i.e. replacing each character in plaintext by other, this chapter discusses digraph techniques i.e. replacing two letters at a time. It start with simple approach of digraph and continue with playfair cipher with it's cryptanalysis. Then it discusses more secure version of playfair called double playfair. At last, the numeric examples is given to grasp the understanding of digraph cipher.

Chapter 6 Apart from ciphers, this chapter discusses about different coding techniques including not-secure (Morse code) and the secure (that used in war). This chapter contains various examples to gets the nut-n-shell of the coding mechanisms.

Chapter 7 This chapter discusses the ciphers that were used in real time by the various spy organizations. It start with stencil cipher, book cipher, Garbo's first & second cipher. The interesting part is the cryptanalysis of respective cipher. Compare to other ciphers, the cryptanalysis of these cipher is more important as they used by spies (thus contain sensitive information). At last, the most secure cipher called one time pad and the reasons why it's not used in regular encipherment techniques.

Chapter 8 As random number playing its key role in ciphers (thus security), this chapter discusses about random number, pseudo-random numbers and the various methods to generate the respective sequence. This chapter divided in two parts i.e. random number generators (like coin spinning, throwing dice, lottery type draws, cosmic rays, etc.) and pseudo-random generators (like linear recurrence, mid square, linear congruence, etc.).

Chapter 9,11 The "Enigma", the name itself enough to get the importance of it. This chapter focuses on the famous enigma machine (used in World War) and it's variants till date. This is one of the unique specialty of book to cover the topic of this much importance. I hope that in future books on cryptography, authors try to explore more on similar topics. In chapter-11, the authors have discussed the various other machines which were used during war with it's architecture.

Chapter 10 Apart from enigma machine, the another cryptographic machine used in World War is the Hagelin cipher machine by various countries. This chapter deals with the Hagelin cipher machine and it's architecture. At last, it discusses the solving approach for the messages encrypted using haglin cipher machine. The cryptographic part is helpful for researcher to do further study in the haglin cipher structures.

Chapter 12,13 All the approaches discusses so far in previous chapters are based on the symmetric key cryptography as sender and receiver requires the same key. However, one of the record breakthrough by inventors (and also Turing award winners) of RSA proposed that one key requires for encryption while another key required during decryption. This phenomenon leads to the public key cryptography (PKC). In this chapters, the author has nicely covered the bricks of PKC. It start with Diffie-Hellman key exchange which is pioneer work towards realizing public key cryptography. In subsequent chapter the famous RSA algorithm for public key cryptography is explained. Finally, it covers the required depths of elliptic curve cryptography for novice readers.

Appendix The author have nicely covered the required knowledge and that too chapter wise in the appendix.

3 Comments and Recommendations

I suggest to considers the example scenarios in ciphers and how the vulnerabilities in it can be exploited. Also, some tools by which one can do such kind of analysis as it also handful for the students and the researchers. This book is the bridge for students to learn about what is security, ciphers and how to exploit it, thus from study to the research. One advancement in this book that I suggest is to add the further findings section in each chapter which specially used by researchers for motivation or guide the further scope in that field. As information security and thus the ciphers is in demand topic in today's world. If some real time example scenario considered than it would be grateful.

While attending the conferences on cryptography I usually gets comment from industry people that who is using this scheme now a day or may be in future. It's like to find a attack in obsolete cipher is less important to that of current ciphers.

On an average, this book gives the undergraduate students (of pre-final year), postgraduate students, researchers, scientists and so on to motivate and also to study further in the security in communication network. Surely, I suggest this book as first hand book in cryptography for UG, PG and the researchers.

The reviewer is a faculty at MEFGI, India.