Review of the book

"Basic Methods of Cryptography"

by Jan C. A. Van Der Lubbe

Cambridge University Press, 1998

ISBN: 978-0521555593

Nishant Doshi
MEFGI, India

1 Summary of the review

I appreciate the way author explains in starting of each chapter, how it relates to previous chapter. The exhaustive analysis of attacks in the chapter 2 is eye catching. The way of explaining topic from the title of book in first chapter is also well defined.

2 Summary of the book

Chapter 1 This is surely an introduction of the book as it precisely written within *nine* pages. It is also admirable as to give the examples for understanding the topic without jumping into deep in the topic.

Chapter 2 This chapter proves that, how utilizable this book is for the beginners in cryptology. The figure 2.1 is helpful to know the analysis of various language is helpful in identifying the catch in respective cipher. In addition, it is nice and helpful that each subtopic start with example to understand the cipher and afterwards how it can be attacked.

Chapter 3 This chapter involves mathematical modeling that helpful to understand the topics of respective chapters. I suggest to read the portion if one is targeting respective chapter.

Chapter 4 This chapter discuss the one of the most known algorithm of its time i.e. DES. It start with what is DES, different modes of it and analysis of it. The *future of DES* is helpful for understanding how and when to utilize it. The International DES is used in PGP, internet and email, this shows that DES is still utilizable at various places.

Chapter 5 This chapter focuses on shift registers. It start with finite state model and generating functions. It also discuses the different properties of shift registers and how it is randomness in nature. Afterwards, it gives the cryptanalysis of LFSRs, which can be helpful for readers to understand, how to study the protocol and how to do cryptanalysis. At last, this chapter covers the part in non-linear shift register.

Chapter 6 This chapter focuses on Public Key Cryptography. The most famous algorithm called RSA , which named after its inventors who got Turing award for this work. This chapter discuss the various alternatives for public key cryptosystem i.e. RSA, knapsack and elliptic curve cryptography. It also discuss the analysis of knapsack and elliptic curve system for public key schemes. Finally, this chapter contains many examples to understand each of public key system in simple way for novice users.

Chapter 7 This chapter discusses the authenticity and integrity of message communication. Chapter start with example scenario of communication between parties and give the attack analysis on that

scenario. It discusses different algorithms like MD5, digital signature,DES hash and so on with its use in achieving the authenticity and integrity of the message.

Chapter 8 This chapter discuses about key management and network security fundamentals. In key management, it discuss how key generate, how to distribute, how to store and how to destruct. It also shows the key distribution in symmetric and asymmetric algorithms. In network security, it shows various encipherment techniques i.e. *link encipherment*,*node encipherment* and *end-to-end encipherment*. At last, the topic of *fair cryptosystem* is eye catching for how to use the cryptosystem in public awareness so thus reducing the usage in criminal activities and so on.

Appendix A This appendix discusses about shannon theory which is backbone for today's security. It is well explained in concise and easy way to the readers.

Appendix B This appendix deals with encipherment of images and videos. It shows the details of how to encipher the image with example and what are the characteristics of it.

3 Comments and Recommendations

Cryptography becomes interesting from ancient times where people hide something and put traps to recover it. This books is great deal of time for understanding the concepts of cryptography. In the cryptography, one question is quite often that, what is the use of respective cryptosystem in today's digital word with powerful machines, unlimited memory, high transfer speed and so on. It would be helpful if in future, one can also give details of current state for respective cryptosystem in the forthcoming books. Also, it would be nice if there is section in chapter which shows the tool to use the respective cryptosystem and also further findings on the respective chapters or topics.

On an average, this book gives the undergraduate students or novice users to motivate and also to study further in the cryptology. Surely, I suggest this book as first hand book for network security and cryptography readers.

The reviewer is a faculty at MEFGI, India.