Review of the book

"The Block Cipher Companion"

by Lars R. Knudsen and Matthey J.B. Robshaw
Springer, 2011

ISBN: 978-3-642-17341-7

Markus Kasper
HGI-Bochum

September 2014

1 Summary of the review

This book is a must read for anyone interested in block cipher cryptanalysis and design. It summarizes the results of the last decades and provides a very good and comprehensible introduction to the topic. The book does not expect any high-level prior knowledge and is well suited for both students and post graduates. Lecturers can use this book as reading material and to copy the clear and simple presentation style with many toy examples for lectures introducing the same topics.

2 What I expected

I asked a colleague of mine for good literature to learn the basics of modern cryptanalysis. What I was looking for is a comprehensible source to learn and understand cryptanalysis techniques such as differential and linear cryptanalysis. As I reply I got the recommendation to study The Block Cipher Companion by Knudsen and Robshaw.

Reading title and backside of the book, I did not expect to find what I was looking for, as the book seemed to be more focused on cipher design. On the other hand it made sense to me to write a good intro to cryptanalysis in a book about block cipher design, and thus I got the book and went through it.

3 Summary of the book

The book starts by introducing basic crypto terminology and providing an overview on the scope of the book. This intro is followed by a summary of the two most important modern block ciphers: The DES and the AES.

The DES chapter starts by describing the primitive and then explains its design features and important properties. Also the variants DESX and 3DES are introduced. While describing and discussing the cipher, the authors put the cipher in its historical context and provide some nice-to-read background information on its development and security.

The Advanced Encryption Standard is introduced in a similar way by starting with a general description of the cipher and it's building blocks followed by state of the art cryptanalytic attacks. The covered attacks illustrate the structural specialties of the AES and explain the existing approaches exploiting them.

Beyond the structural description of the ciphers, their design features and existing attacks, both chapters come with an extensive list of references and further reading material. The authors also provide first figures on differential and linear cryptanalytic results on these ciphers, but the reader first has to understand the later chapters to be able to interprete those numbers.

The fourth chapter provides an overview of the modes of operation and introduces the typical application setups of block ciphers with the corresponding pros and cons. Furthermore many valuable hints such as remarks on IV selection and padding are provided. The authors complete this chapter by summarizing the most important schemes for authentication, hashing and authenticated encryption build from block cipher primitives.

Brute force attacks and time-memory trade-offs are extensively discussed in the following chapter. There, also a short discussion of double- and triple-encryption from a cryptanalyst perspective is provided.

In the subsequent three chapters differential and linear cryptanlysis are first introduced at a basic level and are then discussed in more detail. These three chapters come with about 100 pages and thus provide the material for around 50% of the book.

The intro to differential cryptanalysis covers the main idea, introduces characteristics and differentials and illustrates them at well selected examples. Then the authors illustrate how to use the method to extract key information from a primitive and how to significantly improve the performance of the analysis by employing filtering.

The intro to linear cryptanalysis follows this structure and only introduces the main ideas of linear cryptanalysis and then illustrates its basic application.

These two basic introductory chapters are complemented by a chapter on “advanced topics”. This chapter provides a more detailed coverage of both cryptanalytic methods and introduces , e.g., the differential-linear cryptanalysis approach. Finally the authors provide an extensive discussion on how the results from cryptanalysis impact cipher design and S-Box properties. This section is the most important part for readers interested in the design of block ciphers.

In the last chapter the authors finally discuss the history of block ciphers from DES to AES (and the AES finalists) and the most noticable developments after the AES. A survey of the prominent block ciphers FEAL, IDEA, KASUMI, RC5, Skipjack and PRESENT completes this chapter.

For all chapters many references to further reading material are provided.

4 What you get when reading this book

The book is written very in a very didactic and comprehensible way and provides many examples for most of its content.

The first chapters address readers new to cryptography and without much prior knowledge on block ciphers. The introduction, the chapter on DES, the chapter on AES, the chapter on modes of operation and also the chapter on brute force attacks would be well suited for “Crypto 101” lectures. As I was already familiar with the covered content, I did not learn much reading them. Nevertheless I appreciated the comprehensible presentation style and the extensive references for further reading material. For readers new to cryptography, I expect these chapters to provide a very valuable background.

What I was really interested in were the chapters on differential cryptanalysis, on linear cryptanalysis and the corresponding advanced topics, including the impact on modern cipher design. Starting from close to zero knowledge on cryptanalytic methods I found the introductions very easy to read and to follow. The authors start all topics and by introducing very simple toy examples. For each new concept, the toy examples become a bit more complex to illustrate the new ideas. This strategy allows the authors to transport advanced topics and techniques without asking for too much theoretical background and understanding from the reader.

5 What you do not get when reading this book

The authors do a very good job on focusing on the material they want to transport. Consequently this book does not go into any details of asymmetric cryptography, stream-ciphers or implementation aspects. Personally I think especially implementation aspects are a topic that should be familiar to all designers of cryptographic primitives. Thus I recommend complementing this book by studying works on efficient implementation in hardware and software as well as by a basic intro on implementation attacks.

Also a reader has to keep in mind that cryptanalysis and cipher design is subject to active research, and thus a book can only provide a snapshot of the well understood results at the time of its writing. When considering serious cryptography, i.e. developing own ciphers, it is thus highly recommended to also study the most recent scientific publications on related topics.

6 Recommendation

I've read this book as I was looking for a good intro to cryptanalysis. This is exactly what I got and I recommend this work as an intro to the topic for all interested readers from undergrad students to post-docs. Depending on the reader's prior knowledge, there is no need to hesitate skipping the corresponding chapters. Nevertheless one might learn from the nice way of presenting the content and enjoy the additional reading material. This could be interesting for all lecturers reading the book.

The reviewer is a Ph.D. student of IT-Security and side-channel analysis at the HGI-Bochum.