Review of the book

"Cryptanalytic Attacks on RSA" by Song Y. Yan Springer 2008

ISBN-13: 978-0-387-48741-0

Yuriy R. Aydarov
Perm State University

2009-11-02

1 Summary and first impression

The book is the state of the art encyclopaedia of RSA encryption algorithm. It is well-structured and can be used as lecture notes for any university cryptographic course or student research project. "Cryptanalytic attacks on RSA" includes a notation guide that is very useful for understanding the book by students with different mathematical skills and also for further reading on scientific papers concerning number-theoretic problems. A reader can find all complexity theory and mathematical preliminaries needed in the beginning of the book. Every chapter of "Cryptanalytic attacks on RSA" is concluded by a section "Chapter Notes and Further Reading", in which the author gives a brief overview of all the references which are relevant to the subject. Also, there are plenty of examples in the book.

2 Detailed description

The description of algorithms in "Cryptanalytic attacks on RSA" consists of seven parts:

① **Integer Factorization Attacks.** This chapter consists of classical and modern factorization approaches and their description, namely Fermat factoring algorithm, p+/-1 and ECM algorithms, and several sieve solutions. Their descriptions are very clear and can be easily transformed into source code.

② **Discrete Logarithm Attacks.** In this chapter the author describes Baby-Step Giant-Step, Silver-Pohlig-Hellman, Index and Xedni Calculus algorithms from both practical and theoretical points of view.

③ **Quantum Computing Attacks.** Quantum Computers are inaccessible for most students, scientists and computing professionals, but everybody who is interested in the RSA algorithm should know what would happen if a quantum computer is built one day. In this chapter several quantum algorithms are presented.

④ **Simple Elementary Attacks.** RSA usually is introduced the same way it was made by Rivest, Shamir and Adleman more than thirty years ago. But there are many simple attacks that are known today. This chapter is very useful for students and practitioners who are going to implement the RSA algorithm in some practical environment.

⑤ **Public Exponent Attacks.** From the cryptographer’s point of view, the public exponent in RSA should not be too small. In this chapter, the author explains what does being ’small’ means today. This could be also very useful for understanding of RSA limits.

⑥ **Private Exponent Attacks.** The lower bound of RSA private exponent is presented in this part of the book. Several attacks on small private exponents are described in details.

⑦ **Side Channel Attacks.** These attacks differ greatly from others, but sometimes even more effective than number-theoretic solutions. The subject concludes the description of all attacks known by public.

3 Strengths and Weaknesses, Recommendation

The book has a minor shortcoming, namely it has several errata. This it no problem for an experienced reader, but a little bit confusing for a novice. Also ”Cryptanalytic attacks on RSA” contains a few huge numbers as algorithm data examples, that are very difficult to operate without a computer. However, the book is widely used by the reviewer in Cryptography course in Perm State University, Russia. And a university background of algorithms and mathematics is required for reading this book. It is the most relevant and self-explanatory book about RSA and is very helpful for students and teachers.
In 2010 we are going to publish Russian translation of ”Cryptanalytic Attacks on RSA”.

The reviewer is a Ph.D. student at Perm State university.