

Preface

Cryptographic ciphers come in two flavours: symmetric (AES, etc.) and asymmetric (RSA, etc.). The symmetric ciphers are further divided into block ciphers and stream ciphers. Block ciphers work on large blocks simultaneously (typically comprising 128 or 256 bits) and have no internal state (at least not in their basic version). Stream ciphers work on single bits or single words and need to maintain an internal state to change the cipher at each step.

Typically stream ciphers can reach higher speeds than block ciphers, but their theory is less developed. This is why stream ciphers are often skipped in books on cryptography.

This does not reflect the real importance of stream ciphers. They are used in several everyday applications (for example RC4 is used in wireless LAN and mobile telephones use A5). This book should fill the gap and provide a detailed introduction to stream ciphers.

I wrote this book in the years 2008–2010 when I had a research position at Ghent University.

I want to thank all my colleagues in Ghent for the pleasant time I had there, but especially Prof. Leo Storme who first gave me the opportunity to come to Ghent. We did some nice research together.

I also thank the team of the Springer Verlag who did a great job in improving this book. In addition I want to thank the anonymous referee, without whom the chapter on the Blum-Blum-Shub generator would be missing and there would be no exercises.

Wettenberg, Germany

Andreas Klein



<http://www.springer.com/978-1-4471-5078-7>

Stream Ciphers

Klein, A.

2013, XIX, 399 p. 71 illus., Softcover

ISBN: 978-1-4471-5078-7